univention
be open.

Univention Corporate Server - Handbuch für Benutzer und Administratoren

Release 5.0

30.04.2025

Inhaltsverzeichnis

KAPITEL 1

Einführung

Willkommen im Handbuch für Benutzer und Administratoren von Univention Corporate Server (UCS). Dieses Dokument richtet sich an Systemadministratoren, die UCS betreiben.

1.1 Was ist Univention Corporate Server?

Univention Corporate Server (UCS) ist ein Linux-basiertes Serverbetriebssystem für den Betrieb und die Verwaltung von IT-Infrastrukturen für Unternehmen und Behörden. UCS verwirklicht ein integriertes, ganzheitliches Konzept mit einheitlicher, zentraler Administration. Es kann den Betrieb aller Komponenten in einem zusammenhängenden Sicherheits- und Vertrauenskontext, der so genannten sogenannten UCS-Domäne, gewährleisten. Gleichzeitig unterstützt UCS eine Vielzahl von offenen Standards und verfügt über umfangreiche Schnittstellen zu Infrastrukturkomponenten und Management-Tools anderer Hersteller, so dass es sich in bestehende Umgebungen integrieren lässt.

UCS besteht aus zuverlässiger Open Source Software, die sich in Unternehmen unterschiedlicher Größe bewährt hat. UCS integriert diese Softwarekomponenten über eine einheitliche Web-Schnittstelle. Dies ermöglicht die Integration und Verwaltung des Systems sowohl in einfachen als auch in komplexen verteilten oder virtualisierten Umgebungen.

Dies sind die zentralen Funktionen von UCS:

- Flexibles und umfangreiches Identity- und Infrastrukturmanagementsystem zur zentralen Administration von Servern, Computerarbeitsplätzen, Benutzern und deren Berechtigungen sowie verschiedener Serveranwendungen und Webdienste.
- Dienste zur Integration des Managementsystems in vorhandene Microsoft Active Directory Domänen oder auch für die Bereitstellung dieser Dienste als Alternative zu Microsoft-basierten Serversystemen.
- App Center zur einfachen Installation und Verwaltung von Erweiterungen und Anwendungen.
- Netzwerk- und Intranetdienste zur Verwaltung von DHCP und DNS.
- Datei- und Druckdienste.
- Rechnerverwaltung und Monitoring.
- Maildienste.

Verschiedene Softwarepakete in UCS stellen diese Funktionen bereit, die in diesem Handbuch ausführlich beschrieben werden. Grundsätzlich gehören die in UCS enthaltenen Softwarepakete zu einer der folgenden Hauptkategorien:

1. Basissystem
2. UCS Managementsystem mit Univention Management Console Modulen

3. Das App Center, über das sich zahlreiche weitere Komponenten und Anwendungen anderer Hersteller installieren lassen

Das *Basissystem* umfasst das Betriebssystem der auf der Debian GNU/Linux basierenden und von Univention gepflegten UCS Linux Distribution. Es beinhaltet weitgehend die selbe Software-Auswahl wie Debian GNU/Linux sowie zusätzliche Werkzeuge zur Installation, zur Aktualisierung und zur Konfiguration von Clients und Servern.

Das UCS Managementsystem realisiert einen Single Point of Administration, bei dem ein einziger Verzeichnisdienst die Konten aller Domänenmitglieder verwaltet, z. B. Benutzer, Gruppen und Hosts, sowie Dienste wie DNS und DHCP. Zentrale Komponenten des Verwaltungssystems sind die folgenden Dienste:

- OpenLDAP für den Verzeichnisdienst
- Samba für die Bereitstellung von Domänen-, Datei- und Druckdiensten für Windows
- Kerberos für Authentifizierung und Single Sign-On
- DNS für die Auflösung von Netzwerknamen
- TLS für die sichere Datenübertragung zwischen Systemen

Sie können UCS über eine Weboberfläche, die Univention Management Console-Module oder über die Kommandozeile und in einzelnen Skripten verwenden. Sie können das UCS Managementsystem durch APIs (Programmierschnittstellen) erweitern. UCS bietet eine flexible Client-Server-Architektur, die Änderungen an die beteiligten Systeme überträgt und dort aktiviert.

Über das App Center können Sie zusätzliche Komponenten von Univention und anderen Herstellern installieren. Diese erweitern das System um zahlreiche Funktionen wie Groupware, Dokumentenmanagement und Dienste für Windows, so dass Sie diese auch auf einem UCS-System betreiben und über das UCS-Managementsystem verwalten können.

1.2 Was ist Univention Nubus?

Univention Nubus ist eine Open Source Lösung für die Integration von Identitäts- und Zugriffsmanagement verschiedener Anwendungen. Sie bietet die folgenden Funktionen:

- Verwaltung von Benutzern und Gruppen
- ein Portal mit integriertem Benutzer Self-Service als erste Anlaufstelle für Endnutzer
- zahlreiche Schnittstellen für die Integration von Anwendungen
- gemeinsames Single Sign-On

Standardintegrationen, die auf diesen Schnittstellen basieren, verbinden gängige Anwendungen. Sie finden sie in diesem Handbuch entsprechend gekennzeichnet.

Nubus ist das Univention Produkt für Identitäts- und Zugangsmanagement und das Portal. Sie können Nubus als Teil von UCS oder in einem Kubernetes Cluster betreiben. Univention Corporate Server (UCS) ist eine Möglichkeit, Nubus mit Diensten und Integrationen auf Hardware oder virtuellen Maschinen zu betreiben.

1.3 Überblick über UCS

Linux ist ein Betriebssystem, bei dessen Entwicklung stets Wert auf Stabilität, Sicherheit und die Kompatibilität zu anderen Betriebssystemen gelegt wurde. Dadurch ist es prädestiniert für den Einsatz als stabiles, sicheres und jederzeit verfügbares Serverbetriebssystem.

UCS ist ein auf dieser Basis aufbauendes Serverbetriebssystem, das besonders für den einfachen und sicheren Betrieb sowie die Verwaltung von Anwendungen und Infrastrukturdiensten in Unternehmen und Behörden optimiert wurde. Zur effizienten und sicheren Verwaltung brauchen solche Anwendungen die mit dem UCS Managementsystem realisierte enge Integration mit der Benutzer- und Rechteverwaltung.

UCS kann als die Basis für die IT-Infrastruktur von Unternehmen und Behörden eingesetzt werden und dafür die zentrale Steuerung übernehmen. So leistet es einen wichtigen Beitrag für den sicheren, effizienten und wirtschaftlichen IT-Betrieb. Unternehmenskritische Anwendungen sind in ein einheitliches Konzept integriert, aufeinander abgestimmt und für den professionellen Einsatz vorkonfiguriert. Alternativ lässt es sich auch als Bestandteil vorhandener Microsoft-Domänen betreiben.

1.3.1 Inbetriebnahme

Der Einsatz von UCS beginnt entweder mit einer klassischen Betriebssysteminstallation auf einem physikalischen Server oder als virtuelle Instanz. Weiterführende Informationen finden sich in *Installation* (Seite 9).

1.3.2 Domänenkonzept

In einer mit UCS verwalteten IT-Infrastruktur können sich alle Server, Clients und Benutzer in einem einheitlichen Sicherheits- und Vertrauenskontext, der UCS-Domäne, befinden. Jedem UCS-System wird dazu bei seiner Installation eine so genannte Systemrolle zugewiesen. Mögliche Systemrollen sind Directory Node, Managed Node und Client.

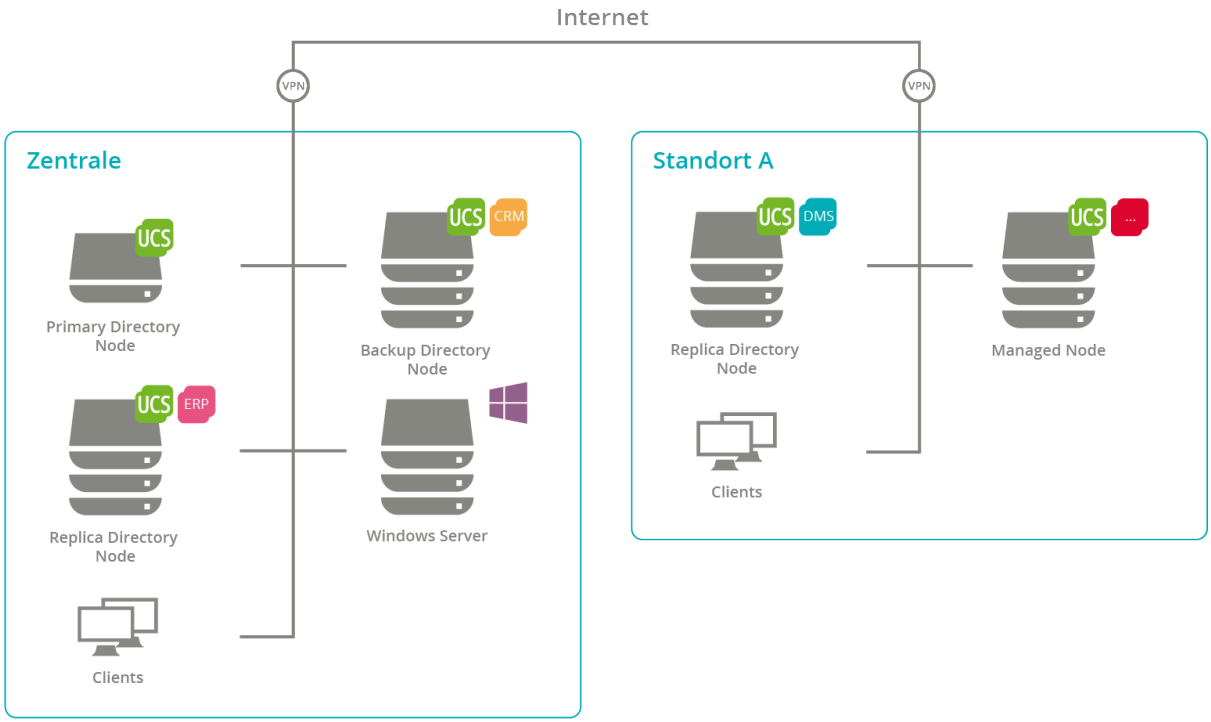


Abb. 1.1: UCS Domänenkonzept

Abhängig von der Systemrolle werden neben dem Betriebssystem grundlegende Dienste wie Kerberos, OpenLDAP, Samba, Module für den Domänenreplikationsmechanismus oder eine Root-CA (Zertifizierungsstelle) auf dem Rechner installiert und automatisch für die gewählte Systemrolle konfiguriert. Eine manuelle Einrichtung jedes einzelnen Dienstes oder Anwendung ist deswegen normalerweise nicht notwendig. Durch den modularen Aufbau und umfangreiche Konfigurationsschnittstellen lassen sich dennoch auf individuelle Bedürfnisse zugeschnittene Lösungen umsetzen.

Durch die Integration von Samba, das den Domänendienst für mit Microsoft Windows betriebene Clients und Server bereit stellt, ist Univention Corporate Server kompatibel zu Microsoft Active Directory (AD), so dass sich das System gegenüber Windows-basierten Systemen wie ein Active Directory Server verhält. Deswegen können beispielsweise Gruppenrichtlinien für Microsoft Windows-Systeme auf die gewohnte Art und Weise verwaltet werden.

Zusätzlich kann UCS auch als Teil einer vorhanden Microsoft Active Directory Domäne betrieben werden. Benutzer und Gruppen aus der Active Directory Domäne können dadurch auf Applikationen des Univention App Centers zugreifen.

Ubuntu- oder macOS-Clients können ebenfalls in eine UCS-Umgebung integriert werden (siehe *Integration von Ubuntu-Clients* (Seite 153)).

1.3.3 Erweiterbarkeit durch das Univention App Center

Das Univention App Center bietet weitere UCS-Komponenten und Erweiterungen sowie eine umfangreiche Auswahl von Softwarelösungen für Business IT-Bereiche wie Groupware, Datenaustausch, CRM oder Backup. Die Anwendungen lassen sich mit wenigen Klicks in bestehende Umgebungen installieren und sind in der Regel einsatzbereit vorkonfiguriert. Sie werden in vielen Fällen direkt in das UCS Managementsystem integriert und stehen anschließend als UMC-Module zur Verfügung. Damit ist eine zentrale Verwaltung von Daten auf Domänenebene gegeben und eine separate Verwaltung, z.B. von Nutzerdaten für unterschiedliche Dienste an unterschiedlichen Orten, entfällt.

1.3.4 LDAP-Verzeichnisdienst

Mit dem UCS Managementsystem können alle Bestandteile der UCS-Domäne über Rechner-, Betriebssystem- und Standortgrenzen hinweg zentral verwaltet werden. Es steht somit ein echter Single-Point-of-Administration für die Domäne zur Verfügung. Ein tragendes Element des UCS Managementsystems ist ein LDAP-Verzeichnis, in dem die domänenweit benötigten, verwaltungsrelevanten Daten vorgehalten werden. Dort wird neben Benutzerkonten und ähnlichem auch die Datenbasis von Diensten wie DHCP gespeichert. Die zentrale Datenhaltung im LDAP-Verzeichnis erspart nicht nur die wiederholte Eingabe derselben Daten, sondern verringert auch die Wahrscheinlichkeit von Fehlern und Inkonsistenzen.

Ein LDAP-Verzeichnis besitzt eine baumartige Struktur, deren Wurzel die so genannte Basis der UCS-Domäne bildet. Die UCS-Domäne realisiert den gemeinsamen Sicherheits- und Vertrauenskontext für ihre Mitglieder. Bei Benutzern begründet ein Konto im LDAP-Verzeichnis die Mitgliedschaft in der UCS-Domäne. Rechner erhalten bei Beitritt in die Domäne ein Rechnerkonto. Auch Microsoft Windows-Systeme können in die Domäne aufgenommen werden, so dass sich Benutzer dort mit ihrem Domänenpasswort anmelden können.

UCS setzt als Verzeichnisdienstserver OpenLDAP ein. Das Verzeichnis wird vom Primary Directory Node bereitgestellt und auf alle anderen UCS Directory Nodes in der Domäne repliziert. Weil ein Backup Directory Node im Notfall den Primary Directory Node ersetzen können soll, wird auf diesen immer das komplette LDAP-Verzeichnis repliziert. Die Replikation auf Replica Directory Nodes kann dagegen mithilfe von ACLs (Access Control Lists) auf beliebige Bereiche des LDAP-Verzeichnisses beschränkt werden, um eine selektive Replikation zu ermöglichen. Dies kann z.B. dann gewünscht sein, wenn Daten aus Sicherheitsgründen auf möglichst wenigen Servern gespeichert werden sollen. Zur sicheren Kommunikation der Systeme innerhalb der Domäne ist in UCS eine Root-CA (Zertifizierungsstelle) integriert.

Weiterführende Informationen finden sich in *LDAP-Verzeichnisdienst* (Seite 36).

1.3.5 Domänenadministration

Der Zugang zum LDAP-Verzeichnis erfolgt über eine webbasierte Benutzerschnittstelle durch Univention Management Console (UMC) Module. Daneben ermöglicht Univention Directory Manager auch die Umsetzung aller domänenweiten administrativen Aufgaben über eine Kommandozeilen-Schnittstelle. Dies eignet sich besonders für die Integration in Skripte oder automatisierte administrative Schritte.

UMC-Module erlauben das Suchen, Anzeigen, Bearbeiten und Löschen von Daten im LDAP-Verzeichnis anhand unterschiedlicher Filter-Kriterien. Die Web-Oberfläche stellt Assistenten bereit u.a. zur Verwaltung von Benutzern, Gruppen, Netzwerken, Rechnern, Verzeichnisfreigaben und Druckern. Die Rechnerverwaltung umfasst auch umfangreiche Funktionen zur Verteilung und Aktualisierung von Software. Über den integrierten LDAP-Verzeichnis-Browser können weitergehende Einstellungen vorgenommen sowie kundenspezifische Objektklassen und Attribute hinzugefügt werden.

Weiterführende Informationen finden sich in *UCS Web-Oberfläche* (Seite 57).

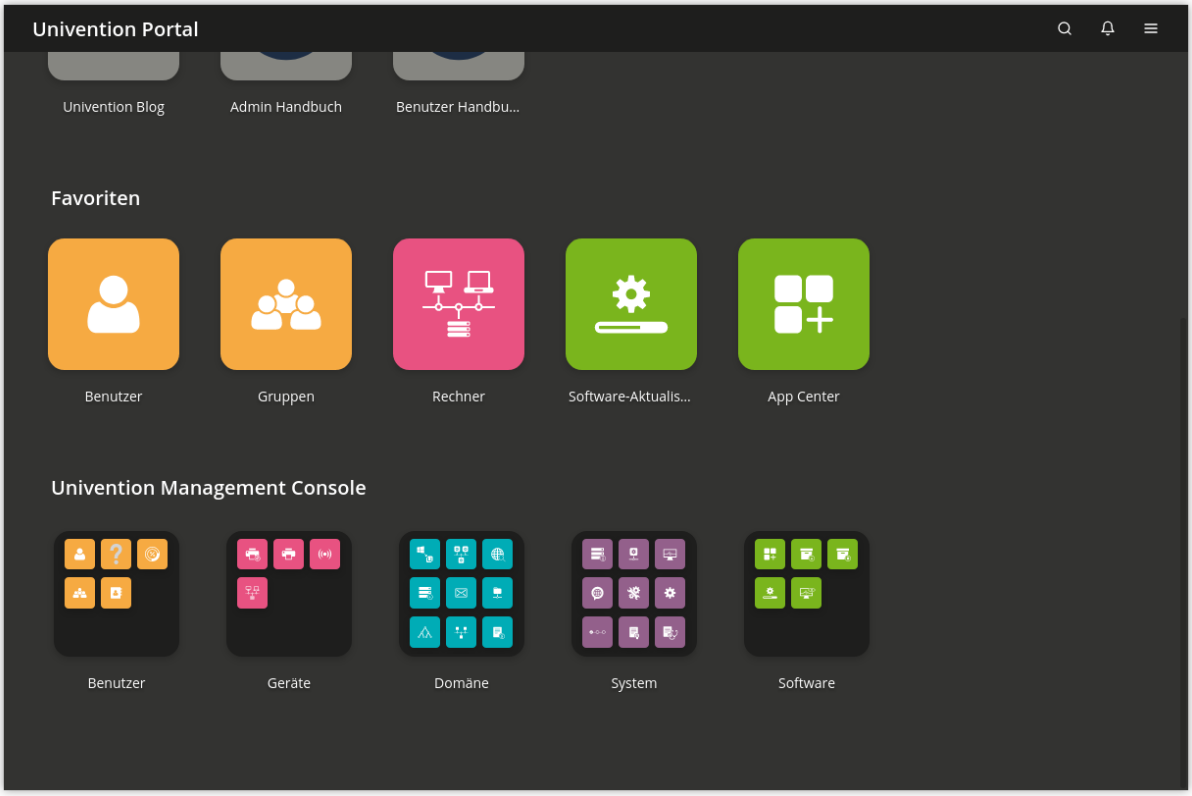


Abb. 1.2: Univention Management Console Module

1.3.6 Rechneradministration

UMC-Module ermöglichen nicht nur den Zugriff auf das LDAP-Verzeichnis, sondern auch die webbasierte Konfiguration und Administration einzelner Rechner. Dazu gehören die Anpassung von Konfigurationsdaten, die Installation von Software sowie die Überwachung und Steuerung von Diensten und dem Betriebssystem an sich. Mit dem UCS Managementsystem ist die Domänenverwaltung sowie die Rechner- und Serverkonfiguration von jedem beliebigen Ort aus über eine komfortable, graphische Web-Oberfläche möglich.

1.3.7 Richtlinienkonzept

Die baumartige Struktur von LDAP-Verzeichnissen ist ähnlich der eines Dateisystems. Sie stellt sicher, dass Objekte (wie z.B. Benutzer, Rechner) sich in einem Container befinden, der wieder in anderen Containern enthalten sein kann. Der Wurzelcontainer wird auch als LDAP-Basis-Objekt bezeichnet.

Richtlinien beschreiben bestimmte administrative Einstellungen, die auf mehr als ein Objekt angewendet werden können. Sie erleichtern die Administration, weil sie an Container gebunden werden können und dann für alle in dem betreffenden Container befindlichen Objekte, sowie die in Unterordnern befindlichen Objekte gelten.

Beispielsweise können Benutzer nach Abteilungszugehörigkeit in unterschiedliche Container oder Organisationseinheiten (die eine besondere Form von Containern darstellen) organisiert werden. Einstellungen wie Bildschirmhintergrund oder aufrufbare Programme können dann mit Hilfe von Richtlinien an diese Organisationseinheiten gebunden werden und gelten für alle unterhalb der betreffenden Organisationseinheit befindlichen Benutzer.

Weiterführende Informationen finden sich in *Richtlinien* (Seite 77).

1.3.8 Listener/Notifier-Replikation

Ein wichtiger technischer Bestandteil des UCS Managementsystems stellt der so genannte Listener/Notifier-Mechanismus dar. Mit ihm lösen das Anlegen, Verändern oder Löschen von Einträgen im LDAP-Verzeichnis definierte Aktionen auf betroffenen Rechnern aus. So führt zum Beispiel das Anlegen einer Verzeichnisfreigabe mit dem UMC-Modul *Freigaben* dazu, das die Freigabe zunächst in das LDAP-Verzeichnis eingetragen wird. Der Listener/Notifier-Mechanismus stellt dann sicher, dass die Konfigurationsdateien auf dem gewählten Server entsprechend erweitert werden und das Verzeichnis im Dateisystem des gewählten Servers erstellt wird, falls es noch nicht existiert.

Der Listener/Notifier-Mechanismus kann leicht um Module für weitere – auch kundenspezifische – Vorgänge ergänzt werden und wird zum Beispiel von zahlreichen Technologiepartnern für die Integration ihrer Produkte in den LDAP-Verzeichnisdienst und das UCS Managementsystem verwendet.

Weiterführende Informationen finden sich in *Listener/Notifier-Domänenreplikation* (Seite 41).

1.4 Weitere Dokumentationen

Dieses Handbuch behandelt nur einen kleinen Ausschnitt der Möglichkeiten von UCS. UCS und auf UCS aufbauende Lösungen bieten unter anderem:

- Umfangreiche Unterstützung für komplexe Serverumgebungen und Replikationsszenarien
- Weitergehende Einsatzmöglichkeiten für Microsoft Windows-Umgebungen
- Zentrales Netzmanagement mit DNS und DHCP
- System- und Netzüberwachung
- Druckserver-Funktionalität
- Proxy-Server

Unter *UCS documentation overview* [1] sind weitere Dokumentationen zu UCS veröffentlicht, die weiterführende Themen behandeln.

1.5 Verwendete Symbole und Konventionen

Im Handbuch werden folgende Symbole verwendet:

Vorsicht: Warnungen werden hervorgehoben.

Bemerkung: Hinweise werden ebenfalls hervorgehoben.

Diese Felder beschreiben den Funktionsumfang eines UMC-Moduls:

Tab. 1.1: Reiter DHCP-Dienst

Attribut	Beschreibung
Name	Ein eindeutiger Name für den DHCP-Dienst.
Beschreibung	Eine beliebige Beschreibung des Dienstes.

Menüeinträge, Schaltflächenbeschriftungen und ähnliches sind *in dieser Schriftform* gesetzt.

Eigennamen sind *hervorgehoben*.

`Computernamen`, `LDAP-DNs`, **`Programmnamen`**, `Dateinamen und -pfade`, `Internetadressen` und `Optionen` werden ebenfalls optisch hervorgehoben.

`Befehle und Tastatureingaben` werden optisch hervorgehoben.

```
Abschnitte aus Konfigurationsdateien, Bildschirmausgaben usw. werden als
Codeblock formatiert.
```

Ein Backslash (`\`) am Ende einer Zeile weist darauf hin, dass der folgende Zeilenumbruch nicht die Bedeutung eines *End-of-Line* hat. Das kommt z.B. bei Befehlen vor, die nicht in einer Zeile des Handbuches dargestellt werden können, an der Kommandozeile aber entweder ohne den Backslash in einem Stück oder mit dem Backslash und einem anschließenden `Enter` eingegeben werden müssen.

Der Weg zu einer Funktion wird ähnlich wie ein Dateipfad dargestellt. *Benutzer ▸ Hinzufügen* bedeutet beispielsweise, dass im Hauptmenü auf *Benutzer* und im erscheinenden Untermenü auf *Hinzufügen* zu klicken ist.

KAPITEL 2

Installation

Die folgende Dokumentation beschreibt die Installation von Univention Corporate Server (UCS). Als Installationsmedium wird eine DVD bereitgestellt. Die Installation erfolgt interaktiv und fragt alle notwendigen System-Einstellungen in einer graphischen Oberfläche ab.

Die Installations-DVD wird für die Rechnerarchitektur *amd64* (64 Bit) bereitgestellt. Die DVD bringt neben einer Unterstützung für die weit verbreiteten BIOS-Systeme auch eine Unterstützung für den Unified Extensible Firmware Interface-Standard (UEFI) mit. Die UEFI-Unterstützung auf der DVD ist auch in der Lage, auf Systemen mit aktiviertem SecureBoot zu starten und UCS dort zu installieren.

Bemerkung: Es ist zu beachten, dass beginnend ab UCS 5.0-0 ein gleichzeitiger Betrieb von UCS und Debian auf einem UEFI System nicht unterstützt wird. Ursache hierfür ist der Bootloader GRUB von Univention Corporate Server, der teilweise die gleichen Konfigurationsdateien wie Debian verwendet. Ein bereits installiertes Debian führt dazu, dass UCS nach der Installation von oder einem Update auf UCS 5.0 nicht (mehr) gebootet werden kann. Eine nachträgliche Installation von Debian wird ebenfalls dazu führen, dass UCS 5.0 nicht mehr gebootet werden kann.

Neben einer Installation auf Hardware oder in einer Virtualisierungslösung kann UCS auch über ein AMI-Image in der Amazon EC2-Cloud installiert werden. Hinweise dazu finden sich in *Installation in der Amazon EC2-Cloud* (Seite 27).

Die Eingabemasken des Installers können mit der Maus oder über die Tastatur bedient werden.

- Mit der `Tab`-Taste kann der Fokus auf das nächste Feld bewegt werden.
- Auf das vorherige Feld wird mit der Tastenkombination `Shift+Tab` gesprungen.
- Mit der `Eingabe`-Taste werden Werte im Eingabefeld übergeben und Schaltflächen betätigt.
- Innerhalb einer Liste oder Tabelle kann mit den *Pfeiltasten* zwischen den Einträgen gewechselt werden.

Bemerkung: Über die Schaltfläche *Abbrechen* kann der aktuelle Konfigurationsschritt abgebrochen werden. Im anschließend angezeigten Menü kann dann ein vorhergehender Konfigurationsschritt erneut ausgewählt werden. Nachfolgende Konfigurationsschritte sind unter Umständen nicht direkt auswählbar, wenn die vorhergehenden Schritte noch nicht vollständig durchlaufen wurden.

2.1 Auswahl des Installationsmodus

Nach dem Starten des Systems vom Installationsmedium erscheint der folgende Bootprompt:

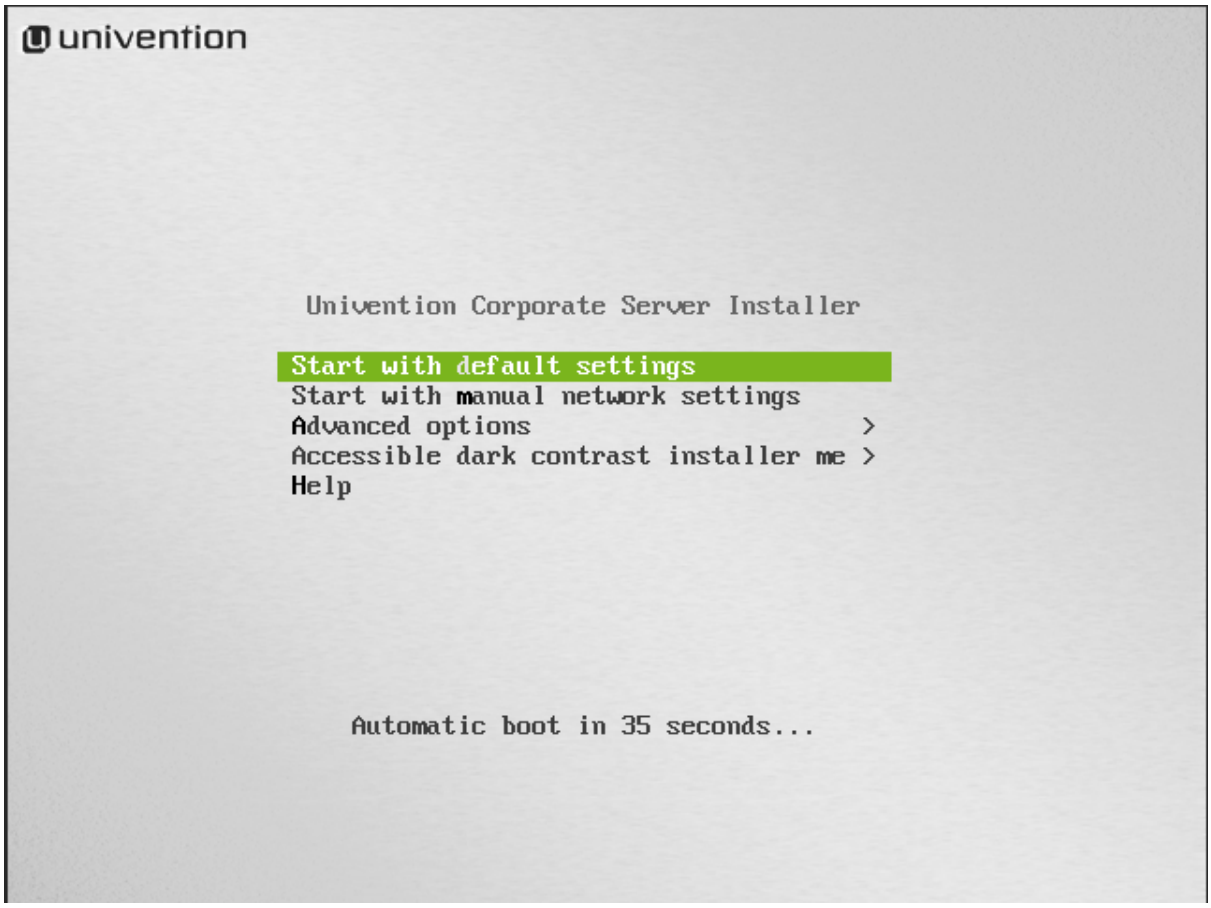


Abb. 2.1: Bootprompt der Installation

Hier kann zwischen verschiedenen Installationsverfahren gewählt werden.

- *Start with default settings* startet die interaktive, graphische Installation von UCS. Bei der Installation fragt das System nach einigen Parametern wie Netzwerkeinstellungen, Festplattenpartitionierung und Domäneneinstellungen für das zu installierende UCS-System und führt anschließend die Installation und Konfiguration durch.
- *Start with manual network settings* führt eine Standardinstallation durch, bei der das Netzwerk nicht automatisch per DHCP konfiguriert wird. Dies ist auf Systemen sinnvoll, wo das Netzwerk manuell eingerichtet werden muss.
- Das Untermenü *Advanced options* bietet die Auswahl fortgeschrittener Optionen für den Installationsprozess:
  - *Start in text mode* führt eine interaktive Standardinstallation im Textmodus durch. Dies ist auf Systemen sinnvoll, die Probleme mit der graphischen Variante des Installers zeigen.
  - *Rescue mode* (Rettungsmodus) ist da, um nicht bootende Systeme wiederherzustellen.
  - *Boot from first hard drive* startet nicht die UCS-Installation, sondern das auf der ersten Festplatte installierte Betriebssystem.
- *Accessible dark contrast installer menu* erlaubt das Starten der Installation in einem dunklen und kontrastreichen Modus.

Nach der Auswahl einer der Installationsoptionen wird der Kernel vom Installationsmedium geladen. Die eigentliche Installation gliedert sich in einzelne Module, die bei Bedarf vom Installationsmedium nachgeladen werden. In einem Modul werden inhaltlich zusammenhängende Einstellungen getroffen, es gibt beispielsweise Module für die Netzkonfiguration oder die Auswahl der zu installierenden Software.

2.2 Auswahl der Installationssprache

Im ersten Schritt wird die Systemsprache ausgewählt, die verwendet werden soll. Die Auswahl beeinflusst die Verwendung von sprachspezifischen Schriftzeichen und ermöglicht die Darstellung von Programmausgaben in den ausgewählten Sprachen im installierten UCS-System.

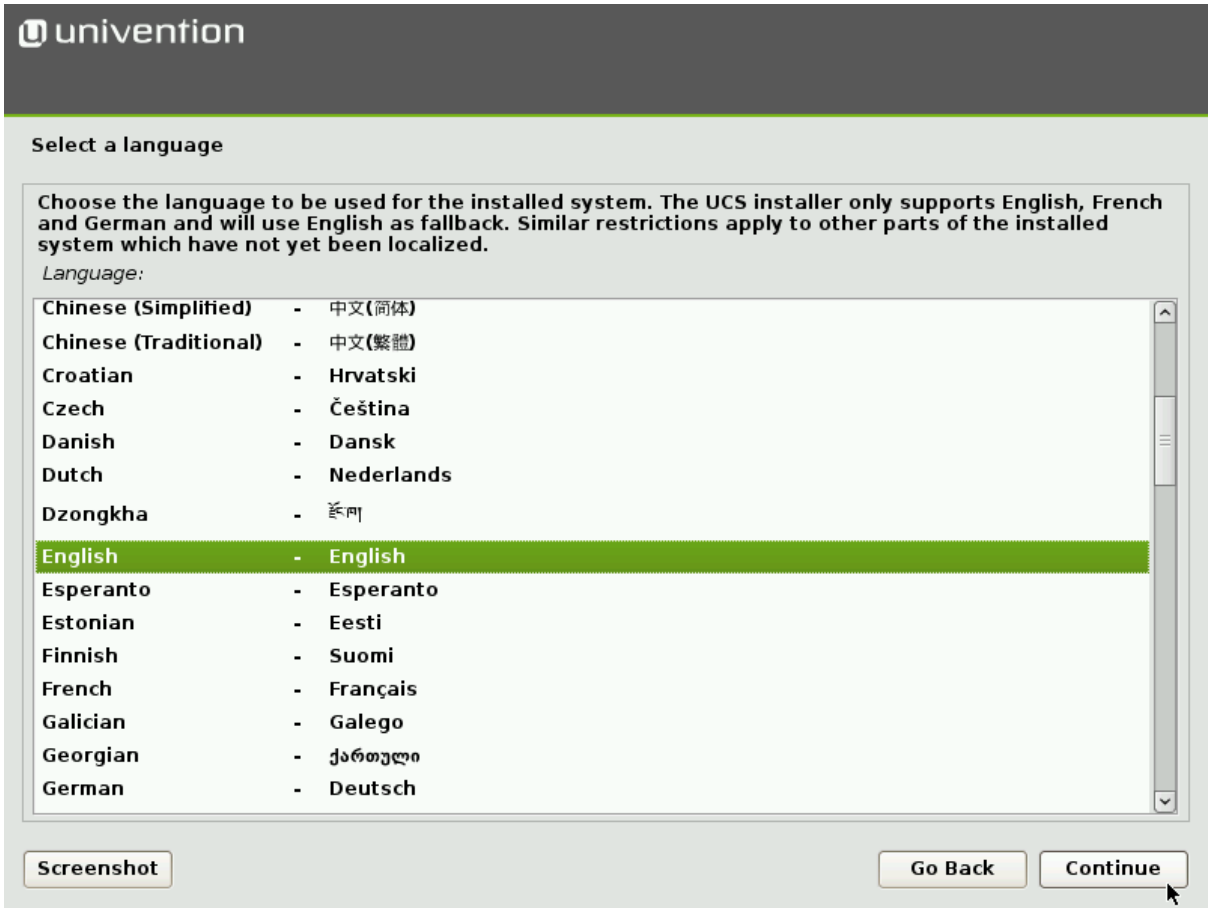


Abb. 2.2: Auswahl der Installationssprache

Sofern der Univention Installer die ausgewählte Sprache unterstützt, wird diese als Installationssprache verwendet, andernfalls wird Englisch verwendet. Derzeit sind Deutsch und Englisch vom Univention Installer unterstützt.

2.3 Auswahl des Standorts

Nach der Auswahl der Systemsprache wird basierend auf der zuvor ausgewählten Sprache eine kleine Liste mit Standorten angezeigt. Wählen Sie aus der Liste einen passenden Standort aus. Der ausgewählte Standort wird verwendet, um z.B. die Zeitzone zu setzen oder den korrekten Sprachdialekt zu ermitteln. Falls kein angezeigter Standort passend sein sollte, kann über den Menüeintrag **weitere** eine umfangreichere Liste angezeigt werden.

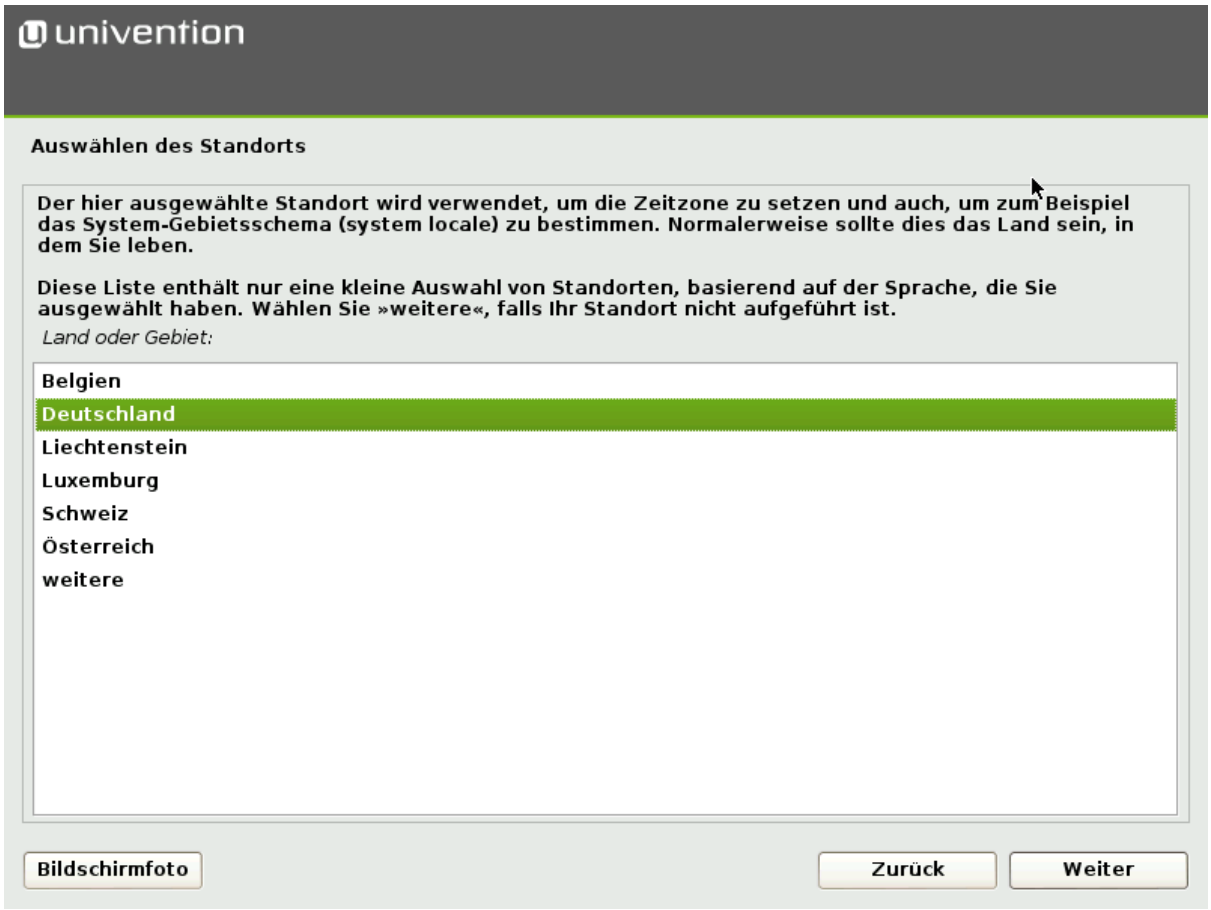


Abb. 2.3: Auswahl des Standorts

2.4 Auswahl der Tastaturbelegung

Unabhängig von der Systemsprache kann ein Tastaturlayout ausgewählt werden. Die hier ausgewählte Sprache sollte zur verwendeten Tastatur passen, das es sonst zu Bedienproblemen kommen kann.

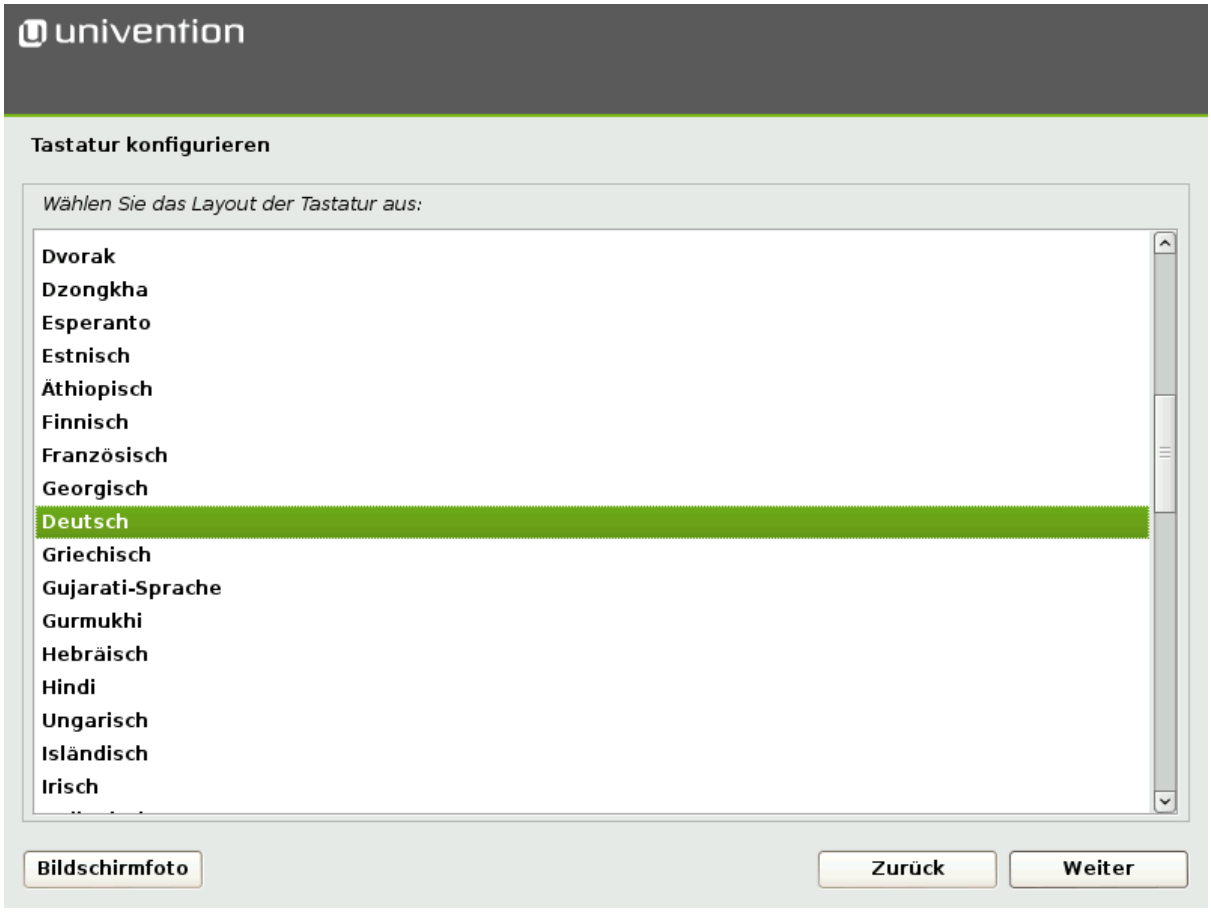


Abb. 2.4: Auswahl der Tastaturbelegung

2.5 Netzwerkkonfiguration

Initial versucht der Univention Installer eine automatische Konfiguration der Netzwerkschnittstellen vorzunehmen. Dies kann durch die Auswahl des Menüeintrags *Start with manual network settings* im Menü des Bootloaders deaktiviert werden. Dabei wird zunächst versucht, eine IPv6-Adresse über die Stateless Address Autoconfiguration (SLAAC) zu ermitteln. Sollte dies nicht erfolgreich sein, versucht der Univention Installer eine IPv4-Adresse über das Dynamic Host Configuration Protocol (DHCP) zu erfragen. Ist dies erfolgreich, wird die manuelle Netzwerkkonfiguration von Univention Installer übersprungen.

Sollte kein DHCP-Server im lokalen Netz vorhanden sein oder es soll eine statische Konfiguration der Netzwerkschnittstelle stattfinden, kann die Schaltfläche *Abbrechen* ausgewählt werden. Der Univention Installer bietet dann an, die automatische Konfiguration zu wiederholen oder die Schnittstelle manuell zu konfigurieren.

Bemerkung: Für die Installation von Univention Corporate Server ist mindestens eine Netzwerkschnittstelle erforderlich. Wird keine unterstützte Netzwerkkarte erkannt, bietet Univention Installer eine Liste der unterstützten Treiber zur Auswahl an.

Bei der manuellen Konfiguration kann für das System wahlweise eine statische IPv4- oder eine IPv6-Adresse angegeben werden. IPv4-Adressen haben 32 Bit Länge und werden in der Regel in vier Blöcken in Dezimalschreibweise

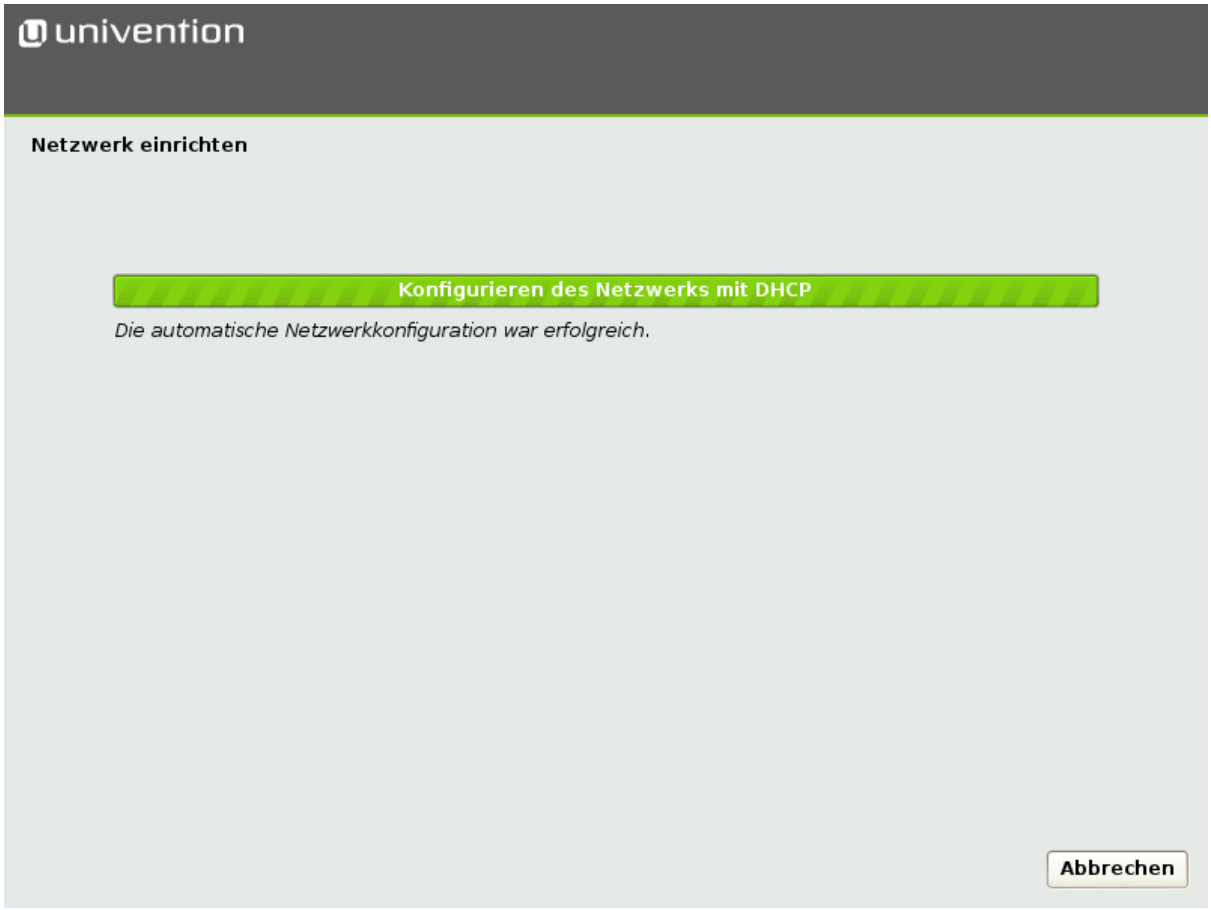


Abb. 2.5: Automatische Netzwerkkonfiguration

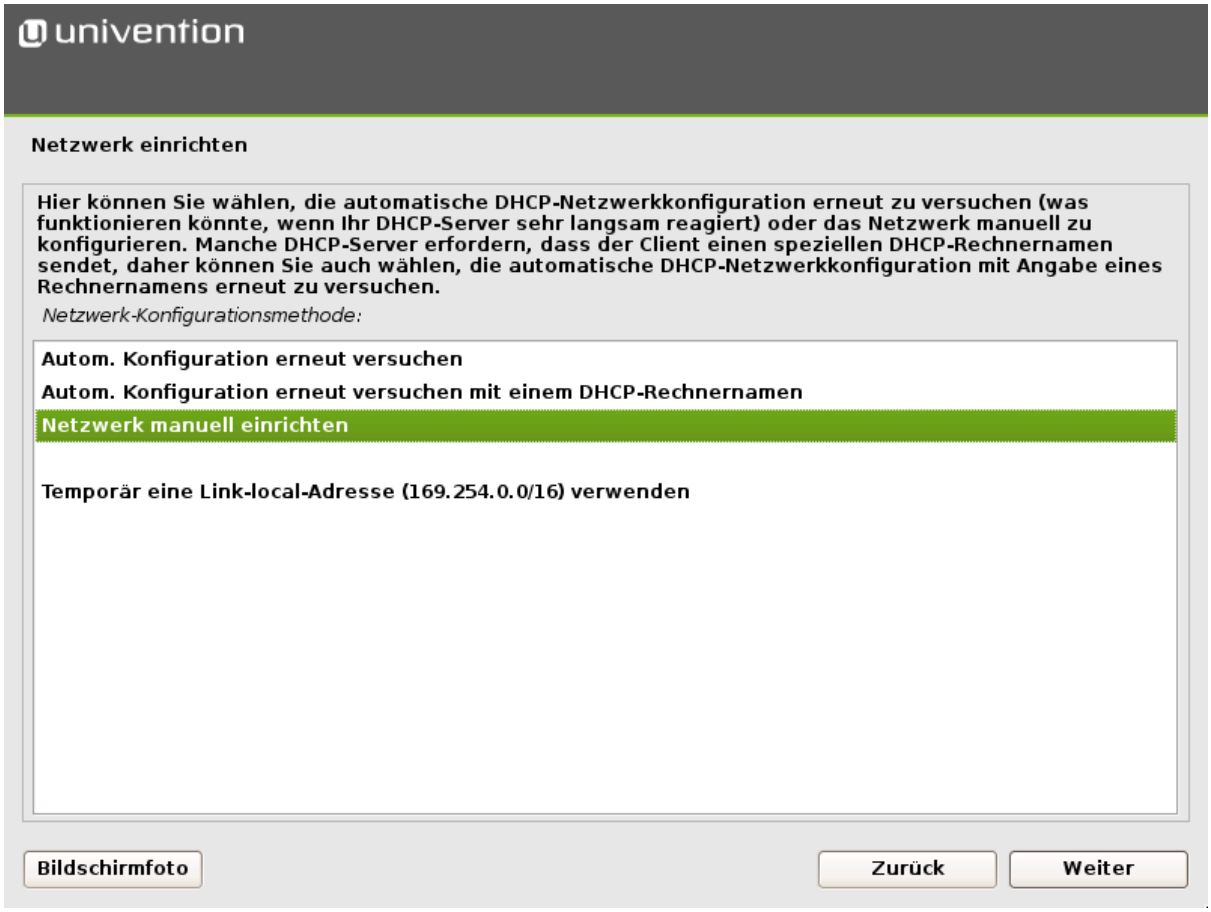


Abb. 2.6: Auswahl der manuellen Netzwerkkonfiguration

dargestellt (z.B. `192.0.2.10`), während IPv6-Adressen vier Mal so lang sind und typischerweise hexadezimal dargestellt werden (z.B. `2001:0DB8:FE29:DE27:0000:0000:0000:000A`). Neben der Angabe einer statischen IP-Adresse werden auch Werte für Netzmaske, Gateway und DNS-Server abgefragt.

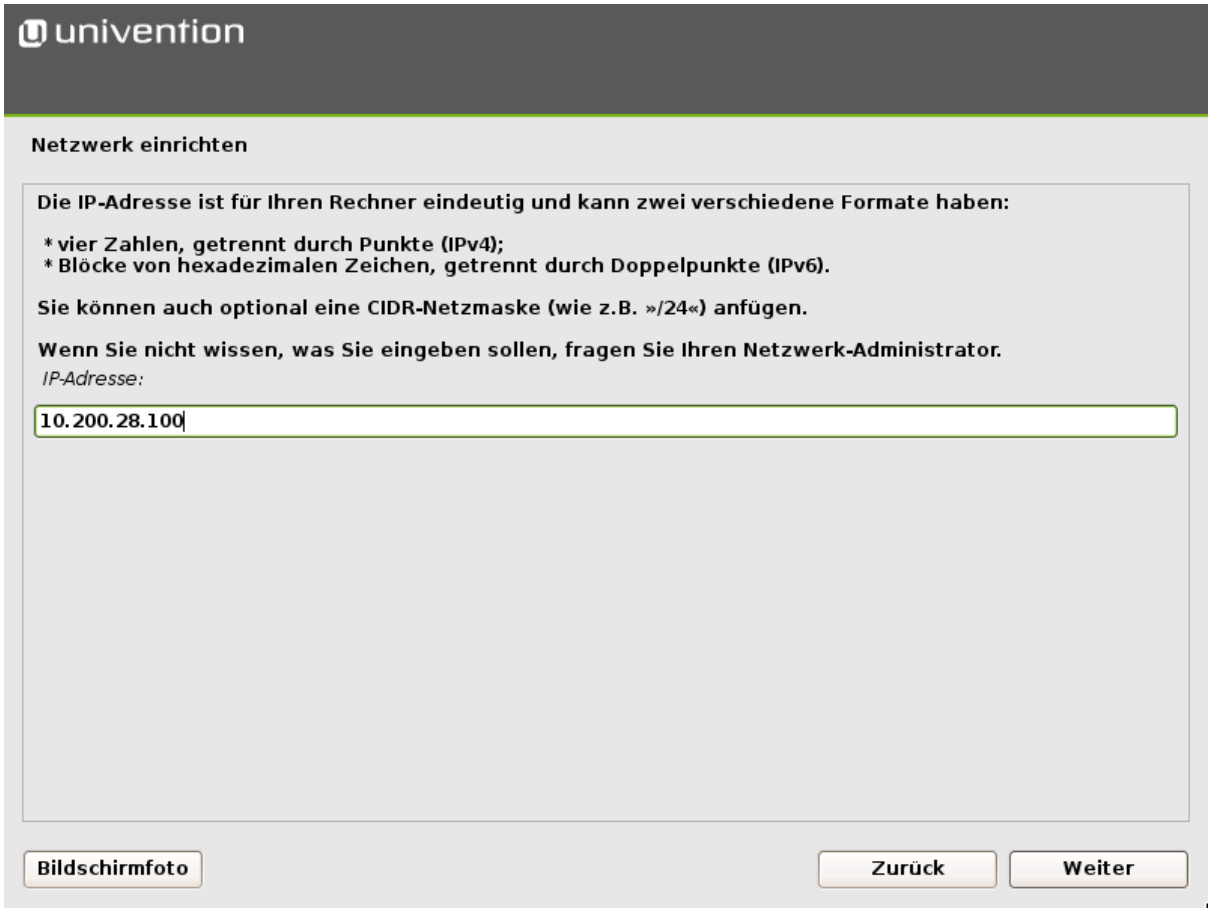


Abb. 2.7: Angabe einer IP-Adresse

Bei der manuellen Angabe eines DNS-Server sind die folgenden Punkte zu beachten. Sie sind abhängig vom späteren Verwendungszweck des UCS-Systems.

- Bei der Installation des ersten UCS-Systems einer neuen UCS-Domäne sollte die IP-Adresse des lokalen Routers (sofern dieser den DNS-Dienst bereitstellt) oder der DNS-Server des Internet-Providers angegeben werden.
- Bei der Installation jedes weiteren UCS-Systems muss als DNS-Server die IP-Adresse eines UCS Directory Nodes angegeben werden. Dies ist notwendig, damit die automatische Erkennung des Primary Directory Node funktioniert. Im Zweifelsfall sollte hier die IP-Adresse des UCS Primary Directory Node angegeben werden.
- Soll das UCS-System während der Installation einer Windows-Active Directory-Domäne beitreten, muss als DNS-Server die IP-Adresse eines Active Directory-Domänencontroller-Systems angegeben werden. Dies ist notwendig, damit die automatische Erkennung des Windows-Active Directory-Domänencontroller funktioniert.

2.6 Einrichtung des root-Passworts

Für die Anmeldung am installierten System ist die Angabe eines Passworts für den Benutzer `root` notwendig. Wird ein Primary Directory Node installiert, wird dieses Passwort auch für den Benutzer `Administrator` eingetragen. Im späteren Betrieb können die Passworte der Benutzer `root` und `Administrator` unabhängig voneinander verwaltet werden. Das Passwort muss im zweiten Feld erneut eingetragen werden.

Das Passwort muss aus Sicherheitsgründen mindestens acht Zeichen umfassen.

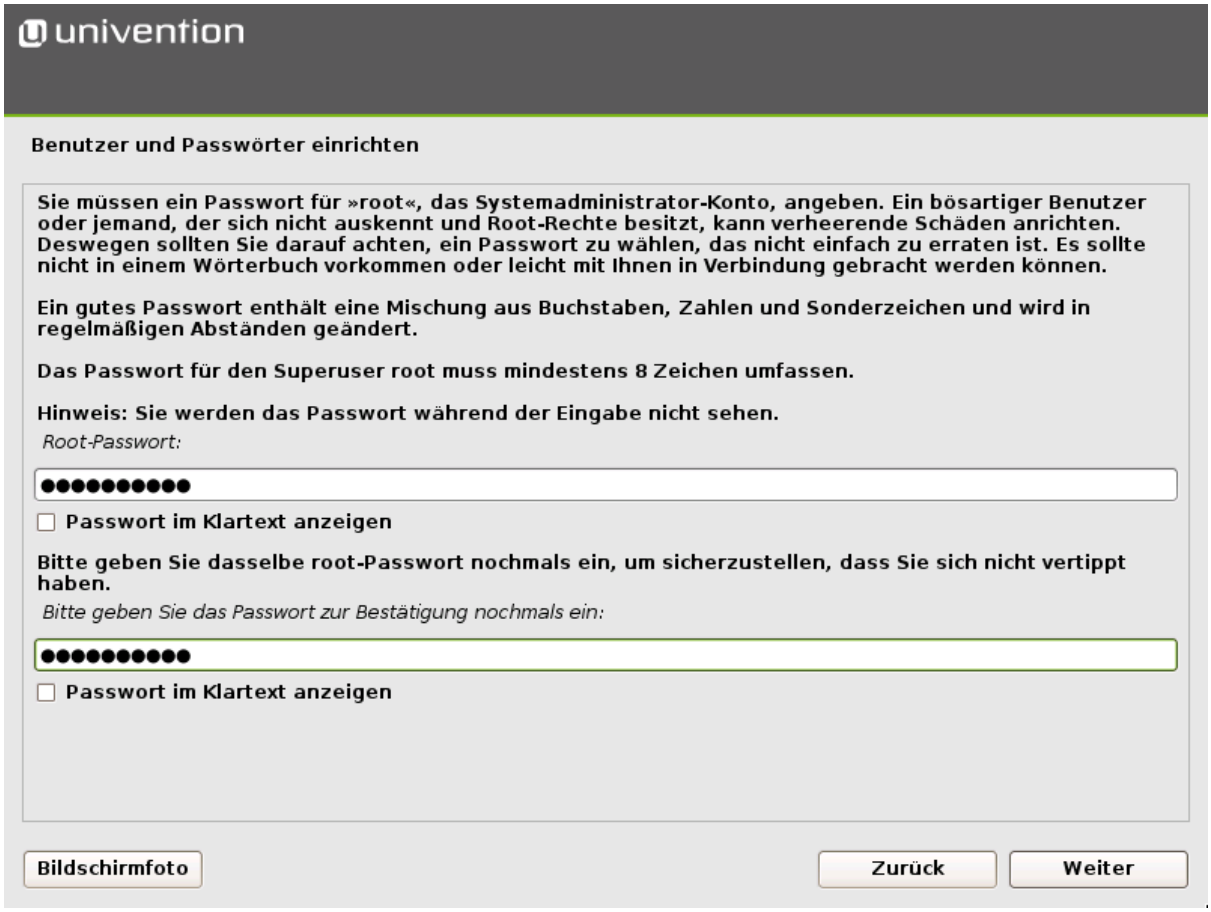


Abb. 2.8: root-Passwort einrichten

2.7 Partitionierung der Festplatten

Der Univention Installer unterstützt die Partitionierung von Festplatten und die Erstellung von unterschiedlichen Dateisystemen (u.a. `ext4` und `XFS`). Darüber hinaus können auch Mechanismen wie der Logical Volume Manager (LVM), RAID oder mit LUKS verschlüsselte Partitionen eingerichtet werden.

Ab UCS 4.0 wählt der Univention Installer automatisch einen passenden Partitionstyp (MBR oder GPT) in Abhängigkeit von der Größe der gewählten Festplatte aus. Auf Systemen mit *Unified Extensible Firmware Interface (UEFI)* wird automatisch die GUID Partition Table (GPT) verwendet.

Zur einfacheren Installation bietet der Univention Installer geführte Installationen an. Bei der geführten Installation werden Standardschemata bezüglich Partitionierung und Formatierung auf die ausgewählte Festplatte angewendet. Darüber hinaus kann auch eine manuelle Partitionierung vorgenommen werden.

Es stehen drei Schemata für eine geführte Partitionierung zur Auswahl:

Geführt - vollständige Festplatte verwenden
: In diesem Schema wird für jedes Dateisystem eine eigene Partition angelegt. Abstraktionsschichten wie LVM

werden nicht verwendet. Im nachfolgenden Schritt wird bestimmt, welche Dateisysteme/Partitionen erstellt werden sollen. Die Größe der Partitionen ist in diesem Schema auf die Größe der jeweiligen Festplatte beschränkt.

Geführt - gesamte Platte verwenden und LVM einrichten
Mit der Auswahl des zweiten Schemas wird auf der ausgewählten Festplatte zunächst eine *Logical Volume Group (LVM)* eingerichtet. Anschließend wird für jedes Dateisystem ein eigenes Logical Volume innerhalb der Volume Group angelegt. Die Größe der Logical Volumes ist bei diesem Schema durch die Größe der Volume Group beschränkt, die später auch durch weitere Festplatten vergrößert werden kann. Im Zweifelsfall wählen Sie dieses Partitionierungsschema.

Geführt - gesamte Platte mit verschlüsseltem LVM
Diese Variante entspricht der vorherigen Variante, allerdings wird zusätzlich die LVM Volume Group verschlüsselt. Dies macht die Angabe des Passwort für die verschlüsselte Volume Group bei jedem Start von UCS notwendig.

Vorsicht: Bei allen drei Varianten gehen die existierenden Daten auf der ausgewählten Festplatte während der Partitionierung verloren!

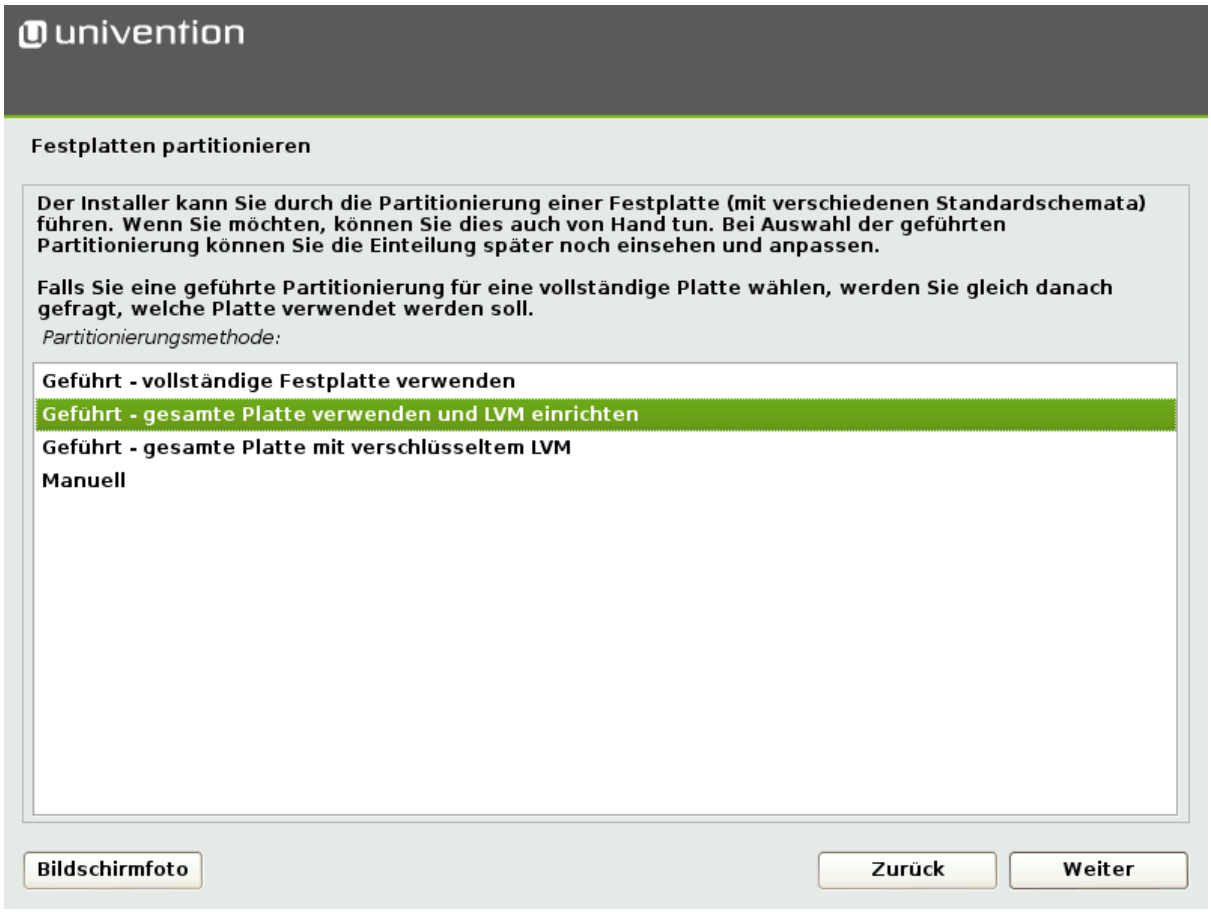


Abb. 2.9: Auswahl des Partitionierungsschemas

Im Anschluss muss aus der Liste der erkannten Festplatte eine ausgewählt werden, auf die die Partitionierungsvariante angewendet werden soll.

Für jede Partitionierungsvariante gibt es drei Untervarianten, die sich in der Anzahl der erstellten Dateisysteme unterscheiden:

Alle Dateien auf eine Partition
Bei dieser Variante wird nur eine Partition oder ein Logical Volume erstellt, auf dem das /-Dateisystem ange-

legt wird.

Separate `/home`-Partition
Neben einem Dateisystem für `/` wird ein weiteres Dateisystem für `/home/` angelegt.

Separate `/home`, `/usr`, `/var` und `/tmp`-Partition
Neben einem Dateisystem für `/` wird für `/home/`, `/usr/`, `/var/` und `/tmp/` jeweils ein eigenes Dateisystem angelegt.

Vor jeder aktiven Änderung auf der Festplatte wird diese noch einmal in einem zusätzlichen Dialog angezeigt und muss explizit bestätigt werden.

Abb. 2.10: Bestätigung von Änderungen auf der Festplatte

Nach Abschluss der Partitionierung werden automatisch das UCS-Grundsystem sowie weitere Software installiert. Dies kann je nach Geschwindigkeit der verwendeten Hardware einige Zeit beanspruchen. Nachfolgend wird das System durch die Installation des GRUB-Bootloaders bootfähig gemacht.

Ein Systemneustart in das frisch installierte System erfolgt anschließend, um darin die Konfiguration abzuschließen.

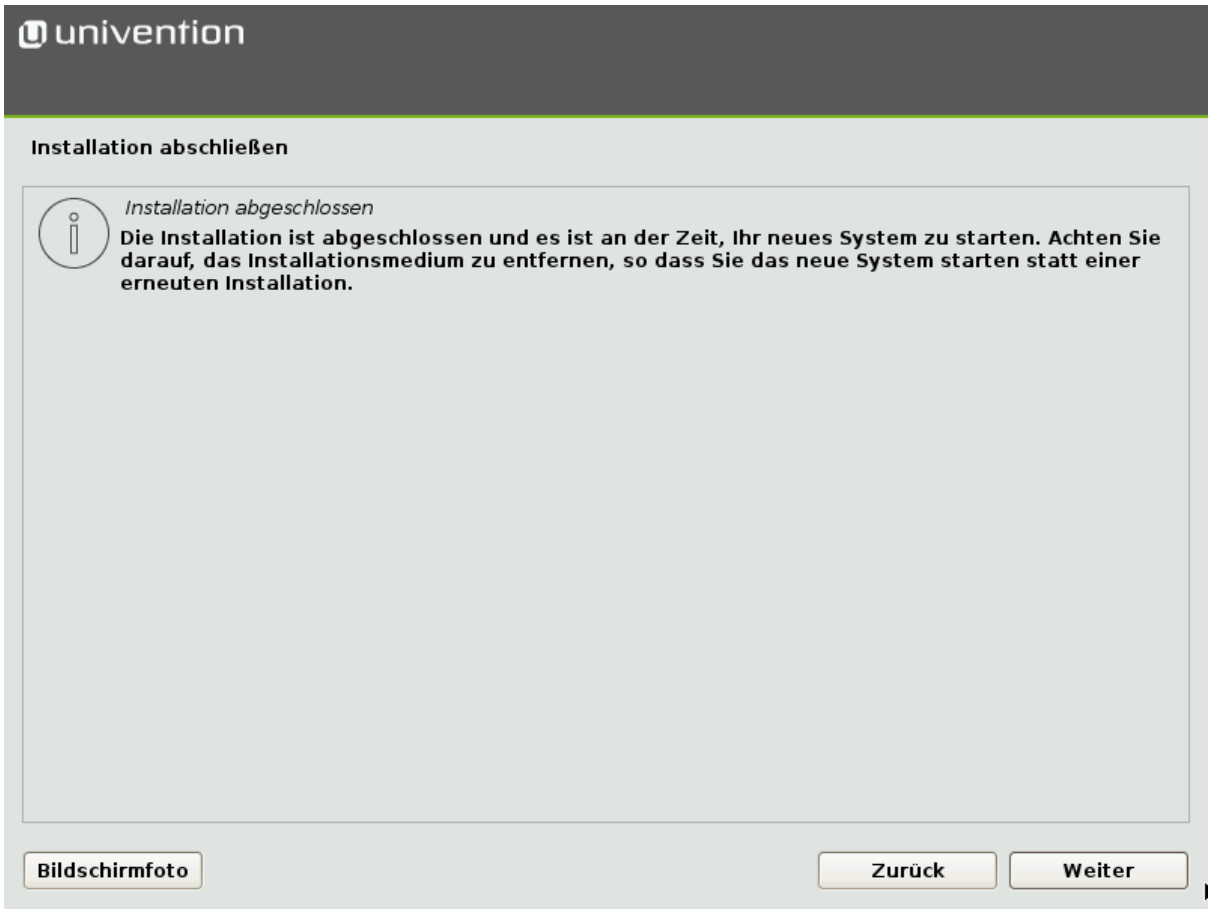


Abb. 2.11: Installation abschließen

2.8 Domäneneinstellungen

Die abschließende Konfiguration des UCS-Systems beginnt mit der Auswahl eines Domänenmodus. Es stehen drei Modi zur Verfügung, die Einfluss auf die nächsten Konfigurationsschritte haben:

Erstellen einer neuen UCS-Domäne
: Im ersten Modus, *Erstellen einer neuen UCS-Domäne*, wird das erste System einer neuen UCS-Domäne konfiguriert: ein UCS-System mit der Systemrolle Primary Directory Node. In den folgenden Konfigurationsschritten werden die notwendigen Informationen zur Einrichtung eines neuen Verzeichnisdienstes, Authentifikationsdienstes sowie DNS-Servers abgefragt. Eine UCS-Domäne kann aus einem einzelnen oder mehreren UCS-Systemen bestehen. Zusätzliche UCS-Systeme können über den Modus *Einer bestehenden UCS-Domäne beitreten* nachträglich aufgenommen werden.

Einer bestehenden Active-Directory-Domäne beitreten
: Dieser Modus, in dem UCS als Mitglied einer Active Directory-Domäne betrieben wird, eignet sich, um eine Active Directory-Domäne um Applikationen zu erweitern, die auf der UCS-Plattform zur Verfügung stehen. Auf der UCS-Plattform installierte Apps sind dann für Benutzer der Active Directory-Domäne nutzbar. Nach der Auswahl dieses Modus werden alle relevanten Informationen für den Beitritt zur Active Directory-Domäne abgefragt und das UCS-System entsprechend konfiguriert.

Einer bestehenden UCS-Domäne beitreten
: Mit der Auswahl des Modus *Einer bestehenden UCS-Domäne beitreten* kann das zu konfigurierende UCS-System einer bereits existierenden UCS-Domäne beitreten. Die UCS-Systemrolle, die es in der Domäne einnehmen soll, wird in einem nachgelagerten Schritt abgefragt.

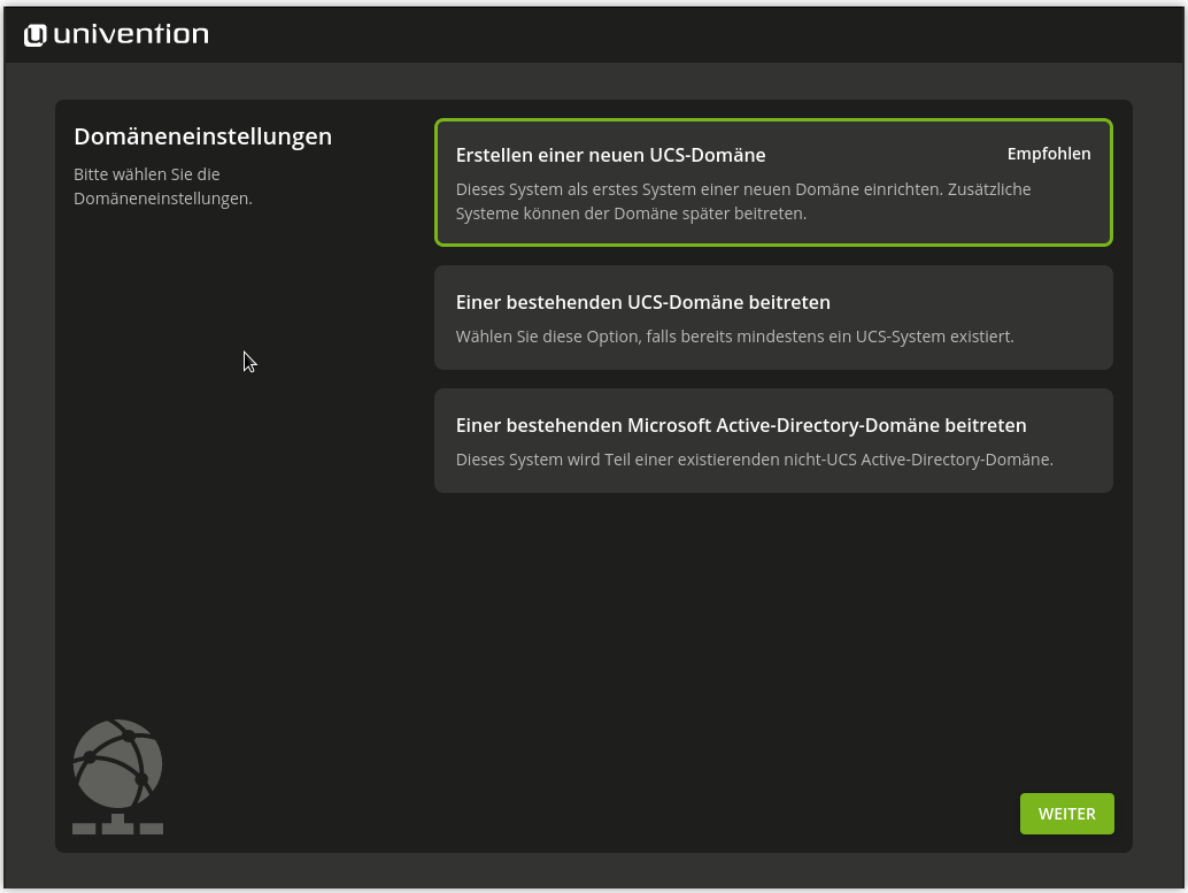


Abb. 2.12: Domäneneinstellungen

2.8.1 Namenskonvention für Rechnernamen

Bei der Einrichtung der Domäne fragt das Domain Setup nach Rechner- und Domänennamen als *voll qualifizierten Domänennamen*. Aus Kompatibilitätsgründen mit Samba 4 und Windows-Domänen muss der Rechnername folgende Namenskonvention erfüllen:

- Länge von 1 bis 13 alphanumerischen Zeichen
- Nur Kleinbuchstaben (`a-z`) und Ziffern (`0-9`)
- Anfang und Ende mit einem alphanumerischen Zeichen und kann dazwischen einen Bindestrich (`-`) enthalten.

Die Namenskonvention hat den folgenden regulären Ausdruck:

```
^[a-z0-9][a-z0-9-]{0,11}[a-z0-9]?$
```

2.8.2 Modus *Erstellen einer neuen UCS-Domäne*

Nach der Auswahl des Modus *Erstellen einer neuen UCS-Domäne* wird in den folgenden zwei Schritten ein *Organisationsname*, eine *E-Mail-Adresse*, ein *vollständiger Rechnername* sowie eine *LDAP-Basis* abgefragt.

Die Angabe eines Organisationsnamens ist optional und wird im zweiten Schritt für die automatische Generierung eines Domänennamens sowie der LDAP-Basis verwendet.

Wird eine gültige E-Mail-Adresse angegeben, wird diese verwendet, um eine personalisierte Lizenz zu aktivieren, die für die Verwendung des Univention App Centers notwendig ist. Die Lizenz wird automatisch generiert und umgehend an die angegeben E-Mail-Adresse zugeschickt. Die Lizenz kann dann über das UMC-Modul *Wilkommen!* eingespielt werden (*Aktivierung der UCS-Lizenz / Lizenz-Übersicht* (Seite 72)).

Aus dem hier eingetragenen vollständigen Rechnernamen (ein Rechnername inklusive Domänenname) wird automatisch der Name des zu konfigurierenden UCS-Systems sowie der Name der DNS-Domäne ermittelt. Aus dem im vorigen Schritt angegebenen Organisationsnamen wird automatisch ein Vorschlag generiert. Es wird empfohlen, keine öffentlich verfügbare DNS-Domäne zu verwenden, da dies zu Problemen in der Namensauflösung führen kann.

Die Namenskonvention für den Rechnernamen finden Sie unter *Namenskonvention für Rechnernamen* (Seite 22).

Für die Initialisierung des Verzeichnisdienstes wird die Angabe einer LDAP-Basis benötigt. Auch hier wird ein Vorschlag automatisch aus dem vollständigen Rechnernamen abgeleitet. In der Regel kann dieser Wert unverändert übernommen werden.

2.8.3 Modus *Einer bestehenden Active-Directory-Domäne beitreten*

Wurde während der Netzwerkkonfiguration der DNS-Server einer Active-Directory-Domäne angegeben, wird im Schritt *Active Directory-Kontoinformationen* automatisch der Name des Active Directory-Domänencontrollers vorgeschlagen. Falls dieser Vorschlag nicht stimmen sollte, kann hier der Name eines anderen Active Directory-Domänencontrollers oder einer anderen Active Directory-Domäne angegeben werden.

Für den Beitritt in die Active Directory-Domäne ist die Angabe eines Active Directory-Kontos sowie des zugehörigen Passworts notwendig. Das Benutzerkonto muss die Berechtigung besitzen, neue Systeme in die Active Directory-Domäne aufzunehmen.

Zusätzlich muss ein Rechnername für das zu konfigurierende UCS-System angegeben werden. Dabei kann der vorgeschlagene Rechnername übernommen oder ein eigener Rechnername eingetragen werden. Der Domänenname des Rechners wird automatisch aus dem Domänen-DNS-Server abgeleitet. In einigen Szenarien (z.B. ein öffentlicher Mailserver) kann es notwendig sein, einen bestimmten vollständigen Rechnernamen zu verwenden. Das UCS-System wird mit dem hier angegebenen Rechnernamen der Active Directory-Domäne beitreten. Der eingerichtete Domänenname kann nach Abschluss der Konfiguration **nicht** mehr verändert werden.

Die Namenskonvention für den Rechnernamen finden Sie unter *Namenskonvention für Rechnernamen* (Seite 22).

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Das erste UCS-System, das einer Active Directory-Domäne beitritt, wird automatisch mit der Systemrolle Primary Directory Node konfiguriert. Wird dieser Modus während der Installation eines weiteren UCS-Systems ausgewählt, wird der Dialog zur

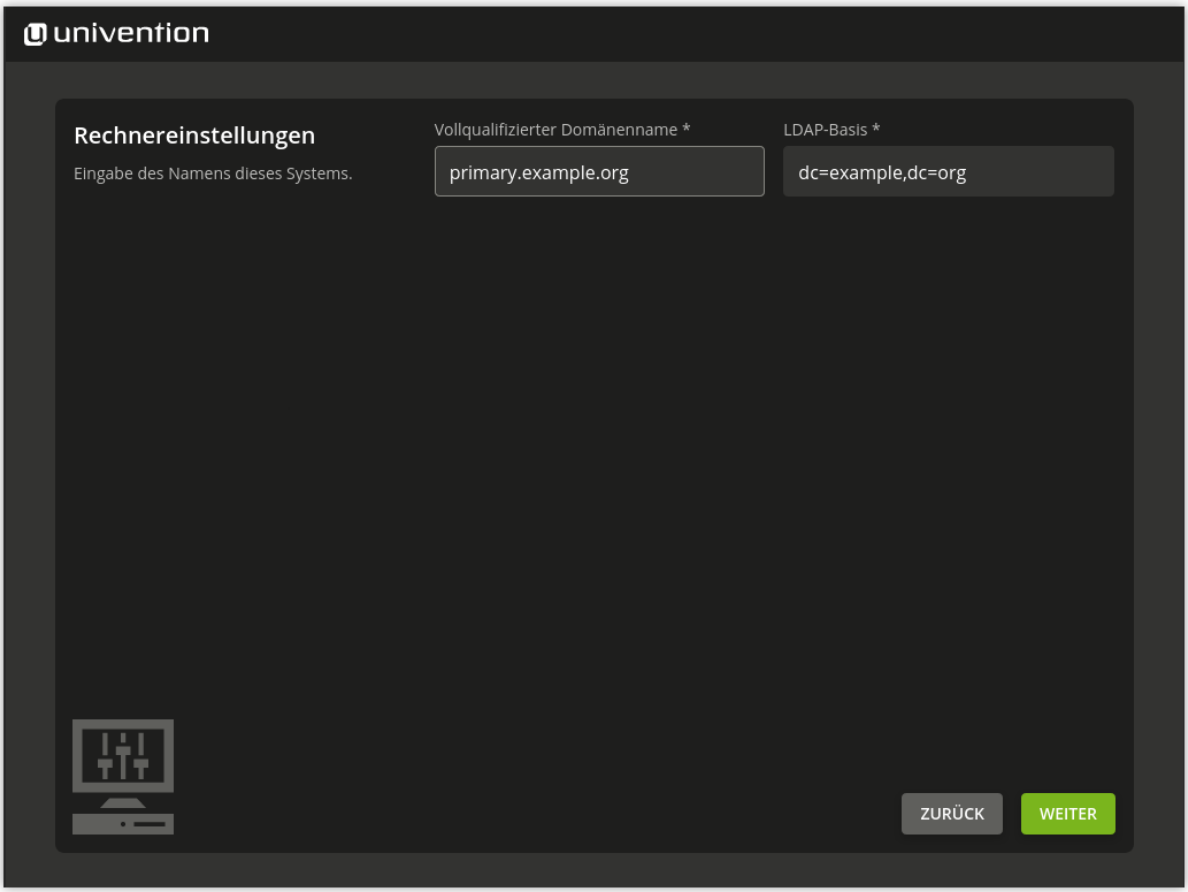


Abb. 2.13: Angabe des Rechnernamens und der LDAP-Basis

Auswahl einer Systemrolle angezeigt. Die einzelnen Systemrollen werden im folgenden Abschnitt genauer beschrieben.

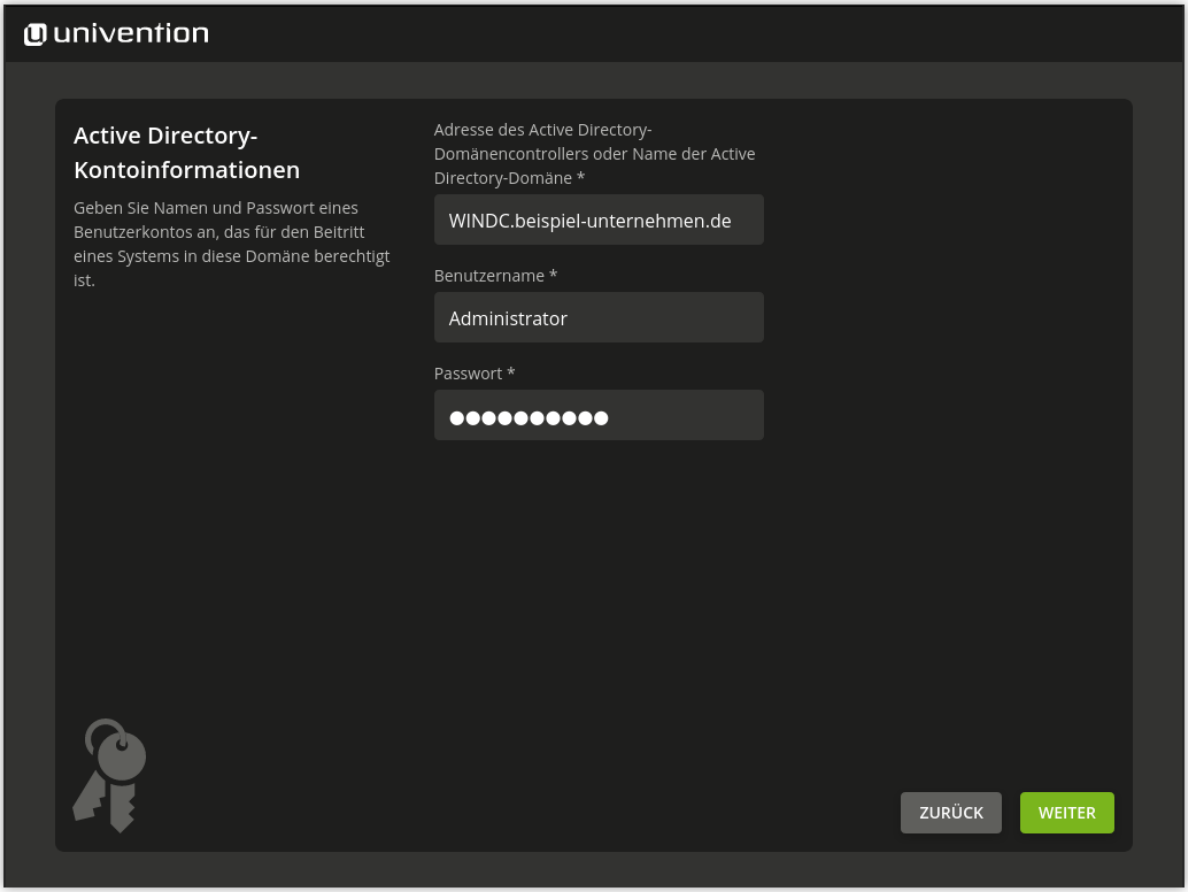


Abb. 2.14: Informationen zum Active Directory-Domänenbeitritt

2.8.4 Modus *Einer bestehenden UCS-Domäne beitreten*

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Das erste System einer UCS-Domäne wird immer mit der Systemrolle Primary Directory Node installiert. Zusätzliche UCS-Systeme können der Domäne später beitreten und mit einer der folgenden Systemrollen konfiguriert werden.

Backup Directory Node
: Der Backup Directory Node dient als Ersatzsystem des Primary Directory Node. Sollte dieser ausfallen, kann ein Backup Directory Node die Rolle des Primary Directory Node dauerhaft übernehmen. Auf Servern mit der Rolle Backup Directory Node werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

Replica Directory Node
: Auf Servern mit der Rolle Replica Directory Node werden die Domänendaten als Nur-Lese-Kopie gespeichert. Im Gegensatz zum Backup Directory Node werden jedoch nicht alle SSL-Sicherheitszertifikate gespeichert. Da die Zugriffe der auf einem Replica Directory Node laufenden Dienste gegen den lokalen LDAP-Verzeichnisdienst erfolgen, bieten sich Replica Directory Nodes für Standortserver und für die Verteilung lastintensiver Dienste an.

Managed Node
: Managed Nodes sind UCS Systeme ohne lokalen LDAP-Verzeichnisdienst. Der Zugriff auf Domänendaten erfolgt hierbei über andere Server der Domäne. Sie eignen sich daher für Dienste, die keine lokale Datenbank für z.B. die Authentifizierung benötigen, beispielsweise Druck- und Dateiserver.

Nach der Auswahl der UCS-Systemrolle werden einige Informationen zum Domänenbeitritt abgefragt. Soll der Domänenbeitritt nicht automatisch während der Installation stattfinden, kann die Option *Domänenbeitritt am Ende der Installation starten* deaktiviert werden. Wurde während der Netzwerkkonfiguration der richtige DNS-Server ausgewählt, kann Univention Installer den Namen des Primary Directory Node automatisch bestimmen. Falls doch in eine andere UCS-Domäne gejoined werden soll, kann die Option *Primary Directory Node im DNS suchen* deaktiviert und der vollständige Rechnername des gewünschten Primary Directory Node im Eingabefeld darunter eingetragen werden. Die für den Domänenbeitritt notwendigen Zugangsinformationen müssen in die beiden Eingabefelder *Administrator-Kontoinformationen* und *Administrator-Passwort*.

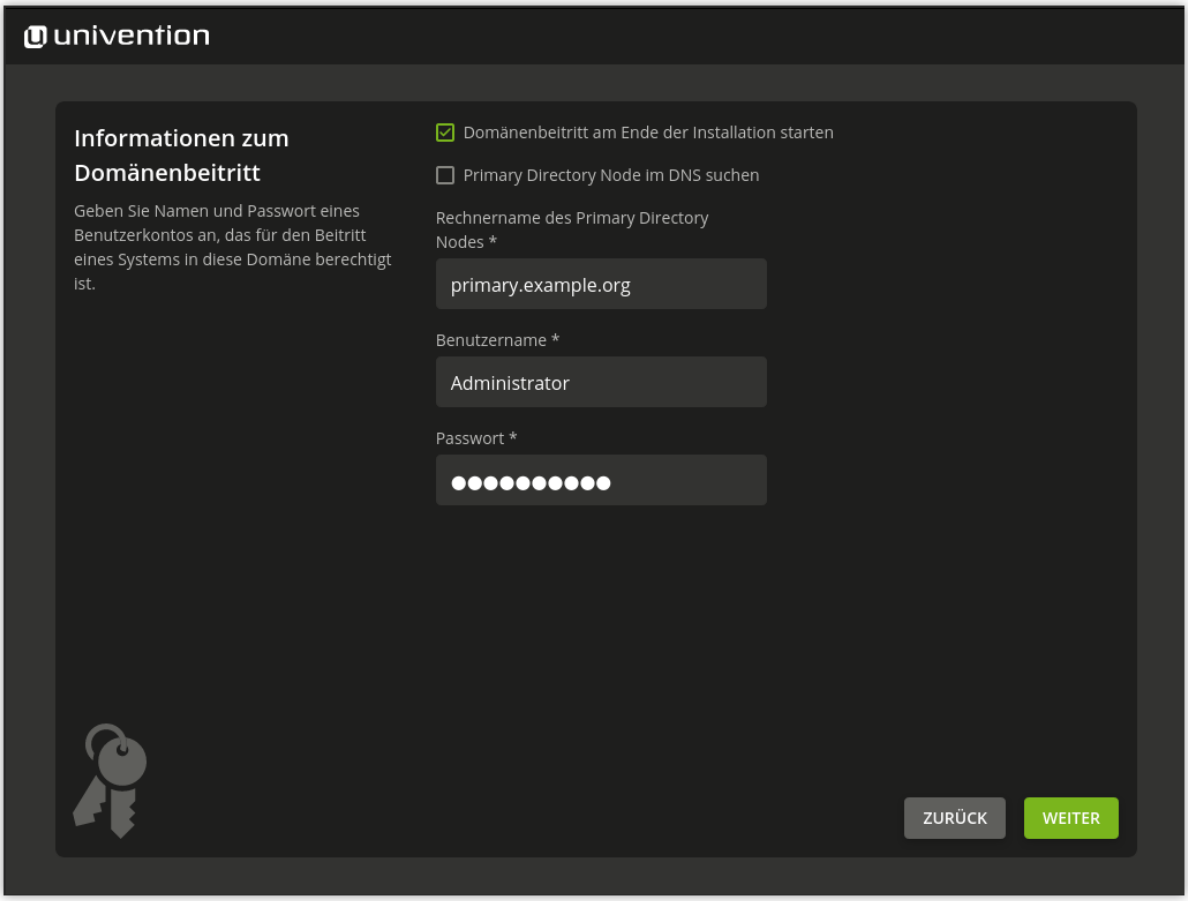


Abb. 2.15: Informationen zum Domänenbeitritt

Im nächsten Schritt muss zusätzlich ein Rechnername für das zu konfigurierende UCS-System angegeben werden. Dabei kann der vorgeschlagene Rechnername übernommen oder ein eigener Rechnername eingetragen werden. Der Domänenname des Rechners wird automatisch aus dem Domänen-DNS-Server abgeleitet. In einigen Szenarien (z.B. ein öffentlicher Mailserver) kann es notwendig sein, einen bestimmten vollständigen Rechnernamen zu verwenden. Der eingerichtete Domänenname kann nach Abschluss der Konfiguration *nicht* mehr verändert werden.

Die Namenskonvention für den Rechnernamen finden Sie unter *Namenskonvention für Rechnernamen* (Seite 22).

2.9 Bestätigen der Einstellungen

In diesem Dialog werden die wichtigsten vorgenommenen Einstellungen angezeigt. Sind alle Einstellungen korrekt, kann über die Schaltfläche *SYSTEM KONFIGURIEREN* die Konfiguration des UCS-Systems veranlasst werden, siehe *Installationsüberblick* (Seite 26).

Mit der Option *System nach der Installation aktualisieren* werden verfügbare Errata-Updates automatisch installiert. Zusätzlich werden auf einem Primary Directory Node alle verfügbaren Patch-Level-Updates und Errata-Updates installiert. Auf allen übrigen Systemrollen werden alle Patch-Level-Updates bis zum Installationsstand des Primary Directory Node eingerichtet. Um den Installationsstand zu prüfen, muss ein Login auf dem Primary Directory Node erfolgen. Dazu werden die in den Join-Optionen angegebenen Anmeldedaten verwendet.

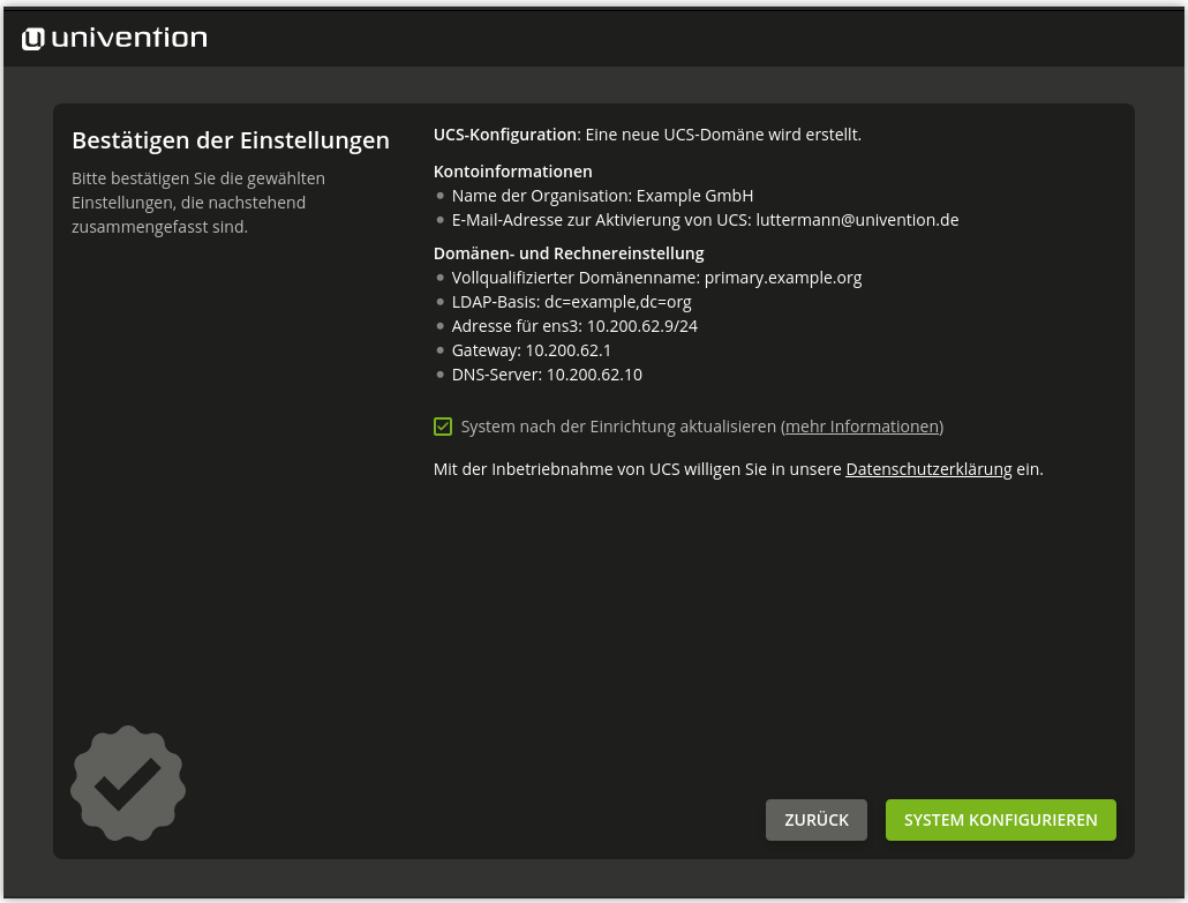


Abb. 2.16: Installationsüberblick

Während der Konfiguration zeigt ein Fortschrittsbalken den Verlauf der Installation an.

Das Installationsprotokoll des Univention Installers wird in den folgenden Dateien abgelegt:

- `/var/log/installer/syslog`
- `/var/log/univention/management-console-module-setup.log`

Der Abschluss der Konfiguration muss über die Schaltfläche *SYSTEM KONFIGURIEREN* bestätigt werden. Das UCS-System wird anschließend auf den ersten vollständigen Bootvorgang vorbereitet und neugestartet.

Das System startet nun von Festplatte. Nach dem Bootvorgang können sich die Benutzer `root` und `Administrator` beim UCS Portal anmelden (siehe *UCS Web-Oberfläche* (Seite 57)), welche unter der während der Installation gesetzten IP-Adresse oder unter dem Rechnernamen erreichbar ist.

Wenn der Rechner als erstes System der UCS-Domäne (Primary Directory Node) installiert wurde, kann nun die Lizenz eingespielt werden (siehe *Aktivierung der UCS-Lizenz / Lizenz-Übersicht* (Seite 72)).

2.10 Fehlersuche bei Installationsproblemen

Hinweise zu eventuellen Installationsproblemen finden sich in der Univention Support Datenbank[2] im Unterpunkt *Installation*.

2.11 Installation im Textmodus

Auf Systemen, die Probleme mit der graphischen Variante des Installers zeigen, kann der Installer auch im Textmodus gestartet werden. Im DVD-Bootmenu *Advanced options* muss dafür der Eintrag *Install in text mode* ausgewählt werden.

Während der Installation im Textmodus werden die gleichen Informationen wie im graphischen Installer angezeigt und abgefragt. Jedoch wird nach der Partitionierung der Festplatten das System auf den ersten Neustart vorbereitet und schließlich neu gestartet.

Nach Abschluss des Neustarts kann die Konfiguration im Webbrowser fortgesetzt werden. Dafür muss im Browser die URL `https://SERVER-IP-ADRESSE` oder `http://SERVER-IP-ADRESSE` aufgerufen werden (HTTPS wird empfohlen). Nach dem Aufruf der Seite ist die Anmeldung mit dem Benutzer `root` erforderlich.

Die Konfiguration im Browser erfragt den Standort sowie die Netzwerkeinstellungen und fährt dann (wie in der graphischen Installation) mit dem Punkt *Domäneneinstellungen* fort, siehe *Domäneneinstellungen* (Seite 21).

2.12 Installation in der Amazon EC2-Cloud

Univention stellt für UCS ein Amazon Machine Image (AMI) für die Amazon EC2 Cloud bereit. Aus diesem generischen Image für alle UCS-Systemrollen wird eine eigene Instanz abgeleitet, die über UMC-Module konfiguriert wird (Domänenname, Softwareauswahl und so weiter).

Die Einrichtung einer UCS-Instanz auf Basis von Amazon EC2 ist in Univention Help 21833 - „Amazon EC2 Quickstart“[3] dokumentiert.

2.13 Installation in VMware

Wird UCS als Gast in VMware installiert muss als *Gastbetriebssystem* die Option *Linux ▸ Debian* ausgewählt werden, weil UCS auf Debian basiert.

Der in UCS verwendete Linux-Kernel bringt alle nötigen Unterstützungstreiber für den Betrieb in VMware direkt mit (`vmw_balloon`, `vmw_pvsci`, `vmw_vmci`, `vmwgfx` und `vmxnet3`).

Die Open-Source-Variante der VMware Tools (Open VM Tools) wird mit UCS ausgeliefert. Die Tools können über das Paket **`open-vm-tools`** installiert werden (sie sind nicht zwingend notwendig, erlauben aber z.B. die Synchronisation der Zeit auf dem Gastsystem mit dem Virtualisierungsserver).

[2] https://help.univention.com/c/knowledge-base/supported/48
[3] https://help.univention.com/t/21833

KAPITEL 3

Domänendienste / LDAP-Verzeichnisdienst

Univention Corporate Server bietet ein plattformübergreifendes Domänenkonzept mit einem gemeinsamen Vertrauenskontext zwischen Linux- und Windows-Systemen. Innerhalb dieser Domäne ist ein Benutzer mit seinem im UCS Managementsystem hinterlegten Benutzernamen und Passwort auf allen Systemen bekannt, und kann für ihn freigeschaltete Dienste nutzen. Das Konto wird über das Managementsystem sowohl für die Windows-Anmeldung als auch für Linux/POSIX-Systeme und Kerberos synchron gehalten. Die Verwaltung von Benutzerkonten ist in *Benutzerverwaltung* (Seite 109) beschrieben.

Alle UCS- und Windowssysteme innerhalb einer UCS-Domäne verfügen über ein Domänenkonto, sobald sie der UCS-Domäne beigetreten sind. Der Domänenbeitritt wird in *Domänenbeitritt* (Seite 30) beschrieben.

Auf dem Primary Directory Node wird die Certificate Authority (CA) der UCS-Domäne betrieben. Dort wird für jedes der Domäne beigetretene System ein SSL-Zertifikat generiert. Weitere Informationen finden sich in *SSL-Zertifikatsverwaltung* (Seite 44).

Jedes Rechnersystem, das Mitglied einer UCS-Domäne ist, besitzt eine Systemrolle. Aus dieser Systemrolle ergeben sich verschiedene Berechtigungen und Einschränkungen, die in *UCS-Systemrollen* (Seite 35) beschrieben sind.

Alle domänenweiten Einstellungen werden in einem Verzeichnisdienst auf Basis von OpenLDAP vorgehalten. In *LDAP-Verzeichnisdienst* (Seite 36) wird beschrieben wie der Speicherumfang durch LDAP-Schema-Erweiterungen ergänzt werden kann, wie eine revisionssichere LDAP-Protokollierung eingerichtet werden kann und wie Zugriffsberechtigungen auf das LDAP-Verzeichnis definiert werden können.

Die Replikation der Verzeichnisdaten innerhalb einer UCS-Domäne erfolgt über den Listener/Notifier-Mechanismus. Weitere Informationen finden sich in *Listener/Notifier-Domänenreplikation* (Seite 41).

Kerberos ist ein Authentifikationsverfahren um in verteilten Netzen über potentiell unsichere Verbindungen eine sichere Identifikation zu erlauben. Jede UCS-Domäne betreibt einen eigenen Kerberosvertrauenskontext (Realm). Weitere Informationen finden sich in *Kerberos* (Seite 45).

3.1 Domänenbeitritt

Ein UCS, Ubuntu- oder Windows-System muss nach der Installation der Domäne beitreten.

Neben UCS, Ubuntu und macOS können auch weitere Unix-Systeme in die Domäne integriert werden. Dies ist in *Extended domain services documentation* [2] beschrieben.

3.1.1 Domänenbeitritt von UCS-Systemen

Es gibt drei Möglichkeiten ein UCS-System einer bestehenden Domäne beitreten zu lassen:

- Direkt am Ende der Installation im Univention Installer, siehe *Modus Einer bestehenden UCS-Domäne beitreten* (Seite 24).
- Nachträglich mit dem Befehl **univention-join**, siehe *Nachträglicher Domänenbeitritt mit univention-join* (Seite 30).
- Durch Verwendung des UMC Moduls *Domänenbeitritt*, siehe *Domänenbeitritt über Univention Management Console Modul* (Seite 31).

Der Primary Directory Node sollte in der Domäne immer auf dem aktuellsten Release-Stand der installiert sein, da beim Join eines Systems in aktuellerer Version gegen einen älteren Primary Directory Node Probleme auftreten können.

Beim Beitritt eines Rechners wird für diesen ein Rechnerkonto angelegt, die SSL-Zertifikate synchronisiert und eine LDAP-Replikation angestoßen. Außerdem werden am Ende des Join-Vorgangs *Join-Skripte* ausgeführt. Diese registrieren anhand der auf dem System installierten Software-Pakete z.B. weitere Objekte im Verzeichnisdienst (siehe *Join-Skripte / Unjoin-Skripte* (Seite 31)).

Der Domänenbeitritt wird auf Client-Seite in der Logdatei `/var/log/univention/join.log` aufgezeichnet, die zur Fehleranalyse herangezogen werden kann. Auf dem Primary Directory Node ausgeführte Aktionen werden in der Logdatei `/home/Join-Account/.univention-server-join.log` abgelegt.

Der Join-Vorgang kann jederzeit wiederholt werden. Nach bestimmten administrativen Schritten (etwa nach Änderungen wichtiger Systemeigenschaften auf dem Primary Directory Node) kann ein erneuter Beitritt der Systeme sogar zwingend erforderlich sein.

Nachträglicher Domänenbeitritt mit *univention-join*

univention-join fragt eine Reihe essentieller Parameter direkt ab, ist aber auch durch mehrere Parameter konfigurierbar:

-dcname <HOSTNAME>

Der Primary Directory Node wird im Regelfall durch eine DNS-Abfrage ermittelt. Wenn das nicht möglich sein sollte (z.B. weil ein Standortserver mit einer abweichenden DNS-Domäne beitreten soll), lässt sich der Rechnername des Primary Directory Node den Parameter `-dcname HOSTNAME` direkt angegeben werden. Der Rechnername muss dabei als vollqualifizierter Name angeben werden, also beispielsweise `primary.firma.de`.

-dcaccount <ACCOUNTNAME>

Als Join-Account wird ein Benutzerkonto bezeichnet, das berechtigt ist, Systeme der UCS-Domäne hinzuzufügen. Standardmäßig ist dies der Benutzer `Administrator` oder ein Mitglied der beiden Gruppen `Domain Admins` und `DC Backup Hosts`. Der Join-Account kann durch den Parameter `-dcaccount ACCOUNTNAME` übergeben werden.

-dcpwd <FILE>

Das Passwort kann durch den Parameter `-dcpwd DATEI` übergeben werden. Das Passwort wird dabei aus der angegebenen Datei ausgelesen.

-verbose

Mit dem Parameter `-verbose` werden zusätzliche Debugausgaben in die Logdateien geschrieben, die die Analyse im Fehlerfall vereinfachen.

Domänenbeitritt über Univention Management Console Modul

Der Domänenbeitritt kann auch webbasiert über das UMC-Modul *Domänenbeitritt* erfolgen. Da auf einem noch nicht der Domäne beigetretenen System der Administrator-Benutzer noch nicht vorhanden ist, muss die Anmeldung am Modul als Benutzer `root` erfolgen.

Wie bei der *Durchführung über die Kommandozeile sind für Domänenbeitritt* (Seite 30) Benutzername und Passwort eines Benutzers notwendig, der berechtigt ist, Rechner der Domäne hinzuzufügen. Ebenfalls wird der Primary Directory Node über eine DNS-Abfrage automatisch ermittelt, kann aber auch explizit im angezeigten Dialogfeld eingetragen werden.

Mit der Option *Erneut beitreten* kann der Domänenbeitritt jederzeit erneut durchgeführt werden.

Join-Skripte / Unjoin-Skripte

Join-Skripte werden während des Domänenbeitritts aufgerufen. Beispiele für von Join-Skripten vorgenommene Änderungen sind die Registrierung eines Druckservers in der Domäne oder die Anpassung von DNS-Einträgen. Die Skripte sind Bestandteil der einzelnen Softwarepakete. Analog dazu gibt es *Unjoin-Skripte*, die nach der Deinstallation einer Softwarekomponente diese Änderungen wieder rückgängig machen.

Join-Skripte werden im Verzeichnis `/usr/lib/univention-install/` und Unjoin-Skripte in `/usr/lib/univention-uninstall/` gespeichert. Jedes Join/Unjoin-Skript verfügt über eine Version. Ein Beispiel: Ein Paket ist bereits installiert und das Join-Skript schon aufgerufen. In der neuen Version des Pakets sind nun zusätzliche Änderungen nötig und die Versionsnummer des Join-Skripts wird erhöht.

Mit dem Befehl **univention-check-join-status** kann geprüft werden, ob Join- oder Unjoin-Skripte aufgerufen werden müssen (entweder weil sie noch nie oder in einer älteren Version aufgerufen wurde).

Nachträgliches Ausführen von Join-/Unjoin-Skripten

Gibt es auf einem System Join- oder Unjoin-Skripte, die noch nicht ausgeführt wurden oder die nur für eine ältere Version ausgeführt wurden, wird beim Öffnen eines UMC-Moduls eine Warnmeldung ausgegeben.

Nicht ausgeführte Join-Skripte können über das UMC-Modul *Domänenbeitritt* aufgerufen werden, in dem der Menüpunkt *Alle Skripte ausführen* aufgerufen wird.

Mit dem Befehl **univention-run-join-scripts** lassen sich alle auf einem System installierten Join-/Unjoin-Skripte ausführen. Ob sie bereits gestartet wurden, prüfen die Skripte selbständig.

Der Name des Join/Unjoin-Skripts und die Skriptausgabe werden auch in `/var/log/univention/join.log` festgehalten.

Wird **univention-run-join-scripts** auf einer anderen Systemrolle als Primary Directory Node ausgeführt, so wird der Benutzer nach einem Benutzernamen und einem Passwort gefragt. Auf dem Primary Directory Node kann dies durch die Option `--ask-pass` erreicht werden.

3.1.2 Windows-Domänenbeitritt

Samba ermöglicht es UCS, dass Microsoft Windows einer UCS-Domäne beitreten kann. Dieser Abschnitt beschreibt den Join-Vorgang am Beispiel von Windows 11, der für andere Windows-Versionen ähnlich ist. Zusätzlich zu den Client Versionen können auch Windows Server-Systeme der Domäne beitreten. Windows Server treten der Domäne als Memberserver bei. UCS unterstützt nicht den Beitritt eines Windows Server-Systems als Domänencontroller. Für weitere Informationen über Windows in einer UCS-Domäne finden Sie unter *Services für Windows* (Seite 177).

Nur domänenfähige Windows-Versionen können der UCS-Domäne beitreten, d.h. ein Domänenbeitritt mit den Home-Versionen von Windows ist nicht möglich.

Beim Domänenbeitritt wird automatisch ein Rechnerkonto für den Windows-Client erstellt (siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 147)). Angaben zu MAC- und IP-Adresse, Netzwerk, DHCP oder DNS können vor oder nach dem Domänenbeitritt durch UMC-Module ergänzt werden.

Der Domänenbeitritt wird in der Regel mit dem lokalen Administrator-Konto des Windows-Systems durchgeführt.

Der Domänenbeitritt dauert einige Zeit und sollte nicht vorzeitig abgebrochen werden. Nach einem erfolgreichen Beitritt erscheint ein kleines Fenster mit der Nachricht *Willkommen in der Domäne <Name Ihrer Domain>*, die mit *OK* bestätigt werden muss. Abschließend muss der Rechner neu gestartet werden, um die Änderungen in Kraft zu setzen.

Domänennamen sollten auf 13 Zeichen beschränkt werden, da diese auf Seite der Windows-Clients ansonsten verkürzt dargestellt werden, was zu Anmeldefehlern führen kann.

Bei einem Domänenbeitritt gegen einen Domänencontroller auf Basis von Samba/AD muss die DNS-Konfiguration des Clients so eingerichtet sein, dass DNS-Einträge aus der DNS-Zone der UCS-Domäne aufgelöst werden können. Außerdem muss die Zeit auf dem Client-System mit der Zeit auf dem Domänencontroller synchronisiert sein.

Unterstütze Windows Versionen

UCS unterstützt die folgenden Microsoft Windows-Versionen, um einer UCS-Domäne beizutreten:

- Windows 10
- Windows 11
- Windows Server in den Versionen 2012, 2016, 2019 und 2022

Windows 11

Der Domänenbeitritt erfordert eine der Editionen *Pro*, *Education*, oder *Enterprise* von Windows 11. Um Windows 11 in eine UCS-Domäne zu joinen, führen sie die folgenden Schritte aus:

1. Um die Windows Systemsteuerung zu öffnen, suchen Sie nach `Systemsteuerung` im Feld *Suchen*.
2. Navigieren Sie in der *Systemsteuerung* zu *System und Sicherheit* ‣ *System* und klicken Sie auf *Domäne oder Arbeitsgruppe*. Wählen Sie *Einstellungen ändern* ‣ *Ändern*.
3. Aktivieren Sie die Option *Domäne*.
4. Geben Sie den Namen der Domäne in das Eingabefeld für den Domain Join ein. Verwenden Sie den vollständigen Domänennamen, zum Beispiel `mydomain.intranet`. Klicken Sie auf die *OK* Schaltfläche.
5. Geben Sie den *Benutzernamen* und das *Passwort* für das Konto eines Domänen Administrators der UCS-Domäne in die entsprechenden Eingabefelder ein. In einer UCS-Domäne ist der Standard-Benutzername des Domänen Administrators `Administrator`.
6. Um den Domänenbeitritt zu starten, klicken Sie auf *OK*.

Windows 10

Der Domänenbeitritt ist nur mit der Pro und Enterprise-Edition von Windows 10 möglich.

Die Systemsteuerung kann über das Suchfeld *Web und Windows durchsuchen*, welches in der Startleiste zu finden ist, gesucht und geöffnet werden. Unter *System und Sicherheit* ‣ *System* muss auf *Einstellungen ändern* ‣ *Ändern* geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld *Domäne* markiert und der Name der Domäne in das Eingabefeld eingetragen werden. Es sollte dabei der vollständige Domänenname verwendet werden, z.B. `mydomain.intranet`. Nach einem Klick auf die Schaltfläche *OK* muss in das Eingabefeld *Benutzername* der Benutzername eines Domänen Administrator, standardmäßig ist dies `Administrator` und in das Eingabefeld *Kennwort* das Passwort des Domänen Administrator eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf *OK* gestartet werden.

Windows Server 2012 / 2016 / 2019 / 2022

Die Systemsteuerung kann erreicht werden, indem der Mauszeiger in die rechte untere Bildschirmecke bewegt wird. Anschließend kann unter *Suchen AR Apps* nach der *Systemsteuerung* gesucht werden. Unter *System und Sicherheit* ‣ *System* muss auf *Einstellungen ändern –> Netzwerk ID* geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld *Domäne* markiert und der Name der Samba-Domäne in das Eingabefeld eingetragen werden. Nach einem Klick auf die Schaltfläche *OK* muss in das Eingabefeld *Name* der Name `Administrator` und in das Eingabefeld *Kennwort* das Passwort von `uid=Administrator,cn=users,` *`Basis-DN`* eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf *OK* gestartet werden.

3.1.3 Ubuntu-Domänenbeitritt

Univention stellt den **`Univention Domain Join Assistant`** für die Integration von Ubuntu-Clients in eine UCS-Domäne bereit. Die Dokumentation und Installationshinweise sind auf Github[4] zu finden.

3.1.4 macOS-Domänenbeitritt

UCS unterstützt den Domänenbeitritt von macOS-Clients in eine UCS-Umgebung mit Samba 4. Diese Anleitung bezieht sich auf macOS 10.8.2.

Der Domänenbeitritt kann über das Systemeinstellungsmenü oder den Kommandozeilenbefehl **`dsconfigad`** erfolgen.

Nach erfolgtem Domänenbeitritt besteht die Möglichkeit CIFS-Freigaben zu definieren, die bei der Anmeldung eines Benutzers unterhalb von `/Volumes` automatisch eingehängt werden. Um dies zu erreichen, muss die folgende Zeile in die Datei `/etc/auto_master` eingefügt werden:

```
/Volumes     auto_custom
```

Außerdem muss die Datei `/etc/auto_custom` angelegt werden und die einzubindenden Freigaben dort in der folgenden Form aufgeführt werden:

```
<SUBFOLDER_NAME>    -fstype=smbfs    ://<FQDN>/<SHARE_NAME>
```

Die eingebundenen Freigaben werden nicht in der Seitenleiste des Finders angezeigt.

[4] https://github.com/univention/univention-domain-join

Domänenbeitritt über das Systemeinstellungen-Menü

In den Systemeinstellungen kann über *Benutzer* das Menü *Anmeldeoptionen* ausgewählt werden. Die Anmeldung erfolgt durch einen Klick auf das Schloss in der linken unteren Ecke, dort muss das lokale Administrator-Konto und dessen Passwort angegeben und *Netzwerk-Account-Server: Verbinden* angeklickt werden.

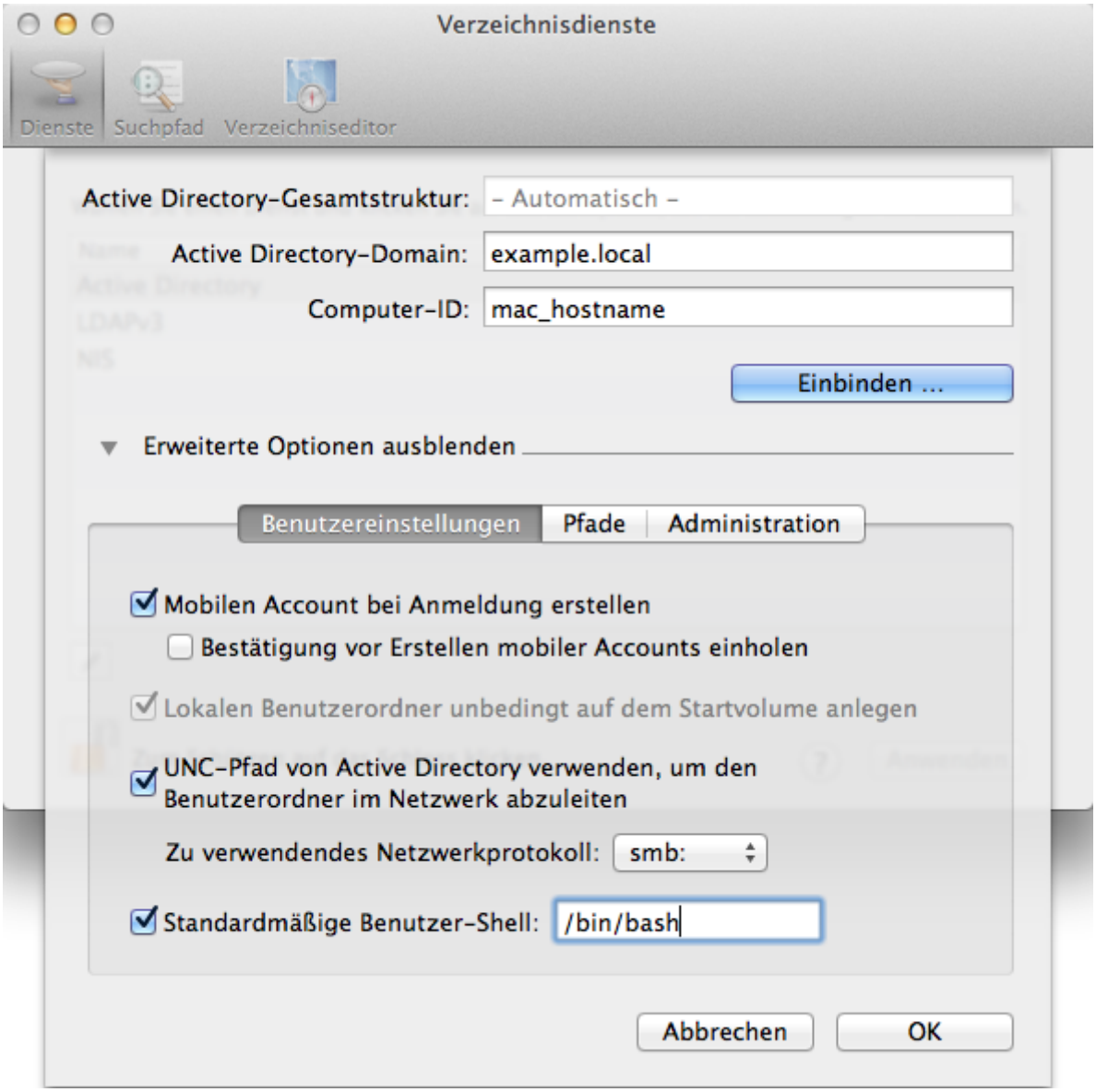


Abb. 3.1: Domänenbeitritt eines macOS-Systems

In den erweiterten Einstellungen sollte die Option *Mobilen Account bei Anmeldung erstellen* aktiviert werden. Sie bietet den Vorteil, das auch ohne Verbindung zur Domäne eine Anmeldung mit der Domänenbenutzerkennung erfolgen kann.

Der Domänenname muss nun im Feld *Active Directory Domain* und der Rechnername des macOS-Clients in das Feld *Computer-ID* eingetragen werden. Der Domänenbeitritt erfolgt nach einem Klick auf *OK*. Für den Domänenbeitritt muss ein Konto aus der Gruppe `Domain Admins` verwendet werden, z.B. `Administrator`.

Domänenbeitritt auf den Kommandozeile

Der Domänenbeitritt kann auch auf der Kommandozeile mit dem Befehl **dsconfigad** erfolgen:

```
$ dsconfigad -a <MAC HOSTNAME> \
  -domain <FQDN> \
  -ou "CN=Computers,<LDAP base DN>" \
  -u <Domain Administrator> \
  -mobile enable
```

Weitere Optionen werden mit **dsconfigad -help** angezeigt.

3.2 UCS-Systemrollen

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Im Folgenden werden die verschiedenen Systemrollen kurz charakterisiert.

3.2.1 Primary Directory Node

Ein System mit der Rolle Primary Directory Node ist das führende System einer UCS-Domäne und wird immer als erstes System installiert. Auf dem Primary Directory Node werden die Domänendaten (wie z.B. Benutzer, Gruppen, Drucker) und die SSL-Sicherheitszertifikate gespeichert.

Kopien dieser Daten werden automatisch auf Server mit der Rolle Backup Directory Node übertragen.

3.2.2 Backup Directory Node

Auf Servern mit der Rolle Backup Directory Node werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

Der Backup Directory Node dient als Ersatzsystem des Primary Directory Node. Sollte dieser ausfallen, kann ein Backup Directory Node die Rolle des Primary Directory Node dauerhaft übernehmen (siehe *Umwandlung eines Backup Directory Node zum neuen Primary Directory Node* (Seite 52)).

3.2.3 Replica Directory Node

Auf Servern mit der Rolle Replica Directory Node werden die Domänendaten als Nur-Lese-Kopie gespeichert. Im Gegensatz zum Backup Directory Node werden jedoch nicht alle SSL-Sicherheitszertifikate gespeichert.

Da die Zugriffe der auf einem Replica Directory Node laufenden Dienste gegen den lokalen LDAP-Datenbestand erfolgen, bieten sich Replica Directory Nodes für Standortserver und für die Verteilung lastintensiver Dienste an.

Ein Replica Directory Node kann nicht zum Primary Directory Node hochgestuft werden.

3.2.4 Managed Node

Managed Node sind Server-Systeme ohne lokalen LDAP-Server. Der Zugriff auf Domänendaten erfolgt hierbei über andere Server der Domäne.

3.2.5 Ubuntu

Ubuntu-Clients können mit einer eigenen Systemrolle verwaltet werden, siehe *Integration von Ubuntu-Clients* (Seite 153).

3.2.6 Linux

Diese Systemrolle wird für die Integration von anderen Linux-Systemen als UCS und Ubuntu verwendet, z.B. für Debian- oder CentOS-Systeme. Die Integration wird in *Extended domain services documentation* [2] beschrieben.

3.2.7 macOS

macOS-Systeme können einer UCS-Domäne mit Samba/AD beitreten. Weitere Hinweise finden sich in *macOS-Domänenbeitritt* (Seite 33).

3.2.8 Domain Trust Account

Ein Domain Trust Account wird für Vertrauensstellungen zwischen Windows und UCS Domänen eingerichtet.

3.2.9 IP-Client

Ein IP-Client ermöglicht die Integration von Nicht-UCS-Systemen in das IP-Management (DNS/DHCP), z.B. für Netzwerkdrucker oder Router.

3.2.10 Windows Domänencontroller

Windows-Domänencontroller in einer Samba/AD-Umgebung werden mit dieser Systemrolle betrieben.

3.2.11 Windows Workstation/Server

Windows-Clients und Windows-Memberserver werden mit dieser Systemrolle verwaltet.

3.3 LDAP-Verzeichnisdienst

Univention Corporate Server speichert domänenweit vorgehaltene Daten in einem LDAP-Verzeichnisdienst auf Basis von OpenLDAP. Dieses Kapitel beschreibt die weitergehende Konfiguration und Anpassung von OpenLDAP.

In einer UCS-Domäne werden oft mehrere LDAP-Server betrieben. Die Konfiguration des/der verwendeten Server(s) wird in *Konfiguration des verwendeten LDAP-Servers* (Seite 170) beschrieben.

Bemerkung: Das LDAP-Verzeichnis ist Teil von Univention Nubus in der *Identity Store and Directory Service* Komponente. Weitere Informationen über Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 2)

3.3.1 LDAP-Schemata

In Schema-Definitionen wird festgelegt, welche Objektklassen existieren und welche Attribute darin enthalten sind - mit anderen Worten, welche Daten in einem Verzeichnisdienst gespeichert werden können. Schema-Definitionen liegen als Text-Dateien vor und werden über die Konfigurationsdatei des OpenLDAP-Servers eingebunden.

UCS verwendet nach Möglichkeit Standard-Schemata, so dass eine Interoperabilität mit anderen LDAP-Applikationen in der Regel gegeben ist. Für Univention-spezifische Attribute - etwa für den Richtlinien-Mechanismus - werden Schema-Erweiterungen mitgeliefert.

LDAP-Schema-Erweiterungen

Um den Aufwand für kleine Erweiterungen im LDAP möglichst gering zu halten, bringt UCS ein eigenes LDAP-Schema für Kundenerweiterungen mit. Die LDAP-Objektklasse `univentionFreeAttributes` kann ohne Einschränkungen für erweiterte Attribute verwendet werden. Sie bringt 20 frei zu verwendende Attribute (`univentionFreeAttribute1` bis `univentionFreeAttribute20`) mit und kann in Verbindung mit jedem beliebigen LDAP-Objekt (z.B. einem Benutzerobjekt) verwendet werden.

Wenn LDAP-Schema-Erweiterungen als Teil von Softwarepaketen ausgeliefert werden sollen, besteht auch die Möglichkeit diese zu paketieren und durch ein Univention Directory Listener-Modul an alle Backup Directory Nodes der Domäne zu verteilen. Weitere Hinweise finden sich in Packaging LDAP Schema Extensions[5].

LDAP-Schema-Replikation

Über den Listener/Notifier-Mechanismus (siehe *Listener/Notifier-Domänenreplikation* (Seite 41)) wird auch die Replikation der LDAP-Schemata automatisiert. Dies entbindet den Administrator von der Notwendigkeit, Schema-Änderungen auf allen OpenLDAP-Servern der Domäne manuell nachzupflegen. Mit der Ausführung der Schema-Replikation vor der Replikation von LDAP-Objekten wird sichergestellt, dass diese nicht aufgrund fehlender Objektklassen oder Attribute scheitert.

Auf dem Primary Directory Node wird beim Start des OpenLDAP-Servers über alle Verzeichnisse mit Schema-Definitionen eine Prüfsumme erzeugt. Diese Prüfsumme wird mit der letzten in der Datei `/var/lib/univention-ldap/schema/md5` gespeicherten Prüfsumme verglichen.

Die eigentliche Replikation der Schema-Definitionen wird vom Univention Directory Listener initiiert. Vor jeder Abfrage einer neuen Transaktions-ID durch den Univention Directory Notifier wird dessen aktuelle Schema-ID abgefragt. Ist diese höher als die Schema-ID auf der Listener-Seite, wird über eine LDAP-Suche vom LDAP-Server des Notifier-Systems dessen aktuell verwendetes Subschema bezogen.

Das ausgelesene Subschema wird auf dem Listener-System im LDIF-Format in die Datei `/var/lib/univention-ldap/schema.conf` eingebunden und der lokale OpenLDAP-Server neu gestartet. Ist die Schema-Replikation mit diesem Schritt abgeschlossen, wird die Replikation der LDAP-Objekte fortgeführt.

3.3.2 Revisionssichere LDAP-Protokollierung

Das Paket **`univention-directory-logger`** ermöglicht die Protokollierung von Änderungen im LDAP-Verzeichnisdienst. Da jeder Datensatz den Hash-Wert des vorhergehenden Datensatzes enthält, können Manipulationen an der Logdatei - etwa entfernte Einträge - aufgedeckt werden.

Um das Paket **`univention-directory-logger`** zu installieren, folgen Sie den Schritten zur Installation von Softwarepaketen auf UCS in *Installation/Entfernung einzelner Pakete über Univention Management Console-Modul* (Seite 105) oder *Installation/Deinstallation von einzelnen Paketen auf der Kommandozeile* (Seite 106).

Einzelne Teilbereiche des Verzeichnisdienstes können von der Protokollierung ausgenommen werden. Diese Zweige können durch die Univention Configuration Registry-Variablen *`ldap/logging/exclude1`* (Seite 309), *`ldap/logging/excludeN`* (Seite 309) konfiguriert werden. Standardmässig ist der Container exkludiert, in dem die temporären Objekte gespeichert werden (`cn=temporary,cn=univention`). Die Protokollierung

[5] https://docs.software-univention.de/developer-reference/5.0/en/ldap.html#settings-ldapschema

der LDAP-Änderungen erfolgt durch ein Univention Directory Listener-Modul. Nach Univention Configuration Registry-Änderungen muss der Univention Directory Listener-Dienst neu gestartet werden.

Die Protokollierung erfolgt in die Datei `/var/log/univention/directory-logger.log` im folgenden Format:

```
START
Old Hash: Hashsumme des vorhergehenden Datensatzes
DN: DN des LDAP-Objekts
ID: Listener/Notifer-Transaktions-ID
Modifier: DN des ändernden Kontos
Timestamp: Zeitstempel im Format dd.mm.yyyy hh:mm:ss
Action: add, modify oder delete

Old Values:
 Liste der alten Attribute, ist leer wenn ein Objekt hinzugefügt wird
New Values:
 Liste der neuen Attribute, ist leer wenn ein Objekt gelöscht wird
END
```

Für jeden protokollierten Datensatz wird eine Hashsumme berechnet und zusätzlich in die Sektion `daemon.info` des Syslog-Dienstes protokolliert.

Ab UCS 4.4 erratum 536[6] wird in der Datei `/var/log/univention/directory-logger.log` vor jede Zeile als Präfix die jeweilige Transaktions-ID des Eintrags hinzugefügt:

```
ID 342: START
ID 342: Old Hash: 70069d51a7e2e168d7c7defd19349985
ID 342: DN: uid=Administrator,cn=users,dc=example,dc=com
ID 342: ID: 342
ID 342: Modifier: cn=admin,dc=example,dc=com
ID 342: Timestamp: 15.04.2020 09:20:40
ID 342: Action: modify
ID 342:
ID 342: Old values:
ID 342: description: This is a description test
ID 342: entryCSN: 20200415091936.317108Z#000000#000#000000
ID 342: modifyTimestamp: 20200415091936Z
ID 342:
ID 342: New values:
ID 342: description: This is a description test
ID 342: entryCSN: 20200415092040.430976Z#000000#000#000000
ID 342: modifyTimestamp: 20200415092040Z
ID 342: END
```

Wurde **`univention-directory-logger`** vor dieser UCS-Version installiert, wird per Default das alte Verhalten (kein Präfix) beibehalten. Durch das Setzen der Univention Configuration Registry Variable *`ldap/logging/id-prefix`* (Seite 309) auf `yes` kann das neue Verhalten aktiviert werden. Dieses Präfix erleichtert eine Korrelation der zusammenhängenden Zeilen bei einer Weiterverarbeitung des Protokolls in Analyse- und Monitoring-Software.

[6] https://errata.software-univention.de/#/?erratum=4.4x536

3.3.3 Timeout für inaktive LDAP-Verbindungen

Mit der Univention Configuration Registry Variable *ldap/idletimeout* (Seite 308) kann ein Zeitraum in Sekunden konfiguriert werden, nach dessen Ablauf eine LDAP-Verbindung serverseitig geschlossen wird. Wenn der Wert auf `0` gesetzt wird, wird kein Ablaufzeitraum angewendet. Der Ablaufzeitraum beträgt standardmäßig sechs Minuten.

3.3.4 LDAP-Kommandozeilen-Tools

Neben den UMC-Modulen gibt es auch eine Reihe von Programmen, mit denen auf der Kommandozeile auf das LDAP-Verzeichnis zugegriffen werden kann.

Das Tool **univention-ldapsearch** vereinfacht die authentifizierte Suche im LDAP-Verzeichnis. Als Argument muss ein Suchfilter übergeben werden, im folgenden Beispiel wird der Administrator anhand der User-ID gesucht:

```
$ univention-ldapsearch uid=Administrator
```

Der Befehl **slapcat** ermöglicht die Speicherung der aktuellen LDAP-Daten in einer Textdatei im LDIF-Format, z.B.:

```
$ slapcat -f /etc/ldap/slapd.conf > ldapdata.txt
```

3.3.5 Zugriffskontrolle auf das LDAP-Verzeichnis

Der Zugriff auf die Informationen im LDAP-Verzeichnis wird serverseitig durch Access Control Lists (ACLs) geregelt. Die ACLs werden in der zentralen Konfigurationsdatei `/etc/ldap/slapd.conf` definiert und über Univention Configuration Registry verwaltet.

Die `slapd.conf` wird dabei durch ein Multifile-Template verwaltet; weitere ACL-Elemente können unterhalb von `/etc/univention/templates/files/etc/ldap/slapd.conf.d/` zwischen den Dateien `60univention-ldap-server_acl-master` und `70univention-ldap-server_acl-master-end` eingefügt oder die bestehenden Templates erweitert werden.

Wenn LDAP-ACL-Erweiterungen als Teil von Softwarepaketen ausgeliefert werden sollen, besteht auch die Möglichkeit diese zu paketieren und durch ein Univention Directory Listener-Modul an alle LDAP-Server der Domäne zu verteilen. Weitere Hinweise finden sich in Packaging LDAP ACL Extensions[7].

Die Grundeinstellung des LDAP-Servers bei Neuinstallationen mit UCS erlaubt keinen anonymen Zugriff auf das LDAP-Verzeichnis. Dieses Verhalten kann mit der Univention Configuration Registry Variable *ldap/acl/read/anonymous* (Seite 308) konfiguriert werden. Einzelne IP-Adressen können über die Univention Configuration Registry Variable *ldap/acl/read/ips* (Seite 308) für den anonymen Lesezugriff freigeschaltet werden.

Nach erfolgreicher Authentifizierung am LDAP-Server können alle Attribute eines Benutzerkontos von diesem Benutzer ausgelesen werden.

Ein zusätzlicher, interner Account, der Root-DN, besitzt darüber hinaus auch schreibenden Vollzugriff.

Unter UCS gibt es außerdem einige standardmäßig installierte ACLs, die den Zugriff auf sensitive Daten unterbinden (z.B. auf das Benutzerpasswort) und für den Betrieb notwendige Regeln setzen (etwa nötige Zugriffe auf Rechnerkonten für Anmeldungen). Der lesende und schreibende Zugriff auf diese sensitiven Daten ist nur für die Mitglieder der Gruppe `Domain Admins` vorgesehen.

Dabei werden auch enthaltene Gruppen unterstützt. Mit der Univention Configuration Registry Variable *ldap/acl/nestedgroups* (Seite 308) kann diese Gruppen-in-Gruppen-Funktionalität für die LDAP-ACLs deaktiviert werden, wodurch eine Geschwindigkeitssteigerung bei den Verzeichnisdienstanfragen zu erwarten ist.

[7] https://docs.software-univention.de/developer-reference/5.0/en/ldap.html#settings-ldapacl

Delegation des Zurücksetzens von Benutzerpasswörtern

Um einer Teilgruppe von Administratoren mit eingeschränkten Rechten, z.B. einem Helpdesk, das Zurücksetzen von Benutzerpasswörtern zu ermöglichen, kann das Paket **univention-admingrp-user-passwordreset** installiert werden. Es legt über ein Join-Skript die Benutzergruppe `User Password Admins` an, sofern diese noch nicht existiert.

Mitglieder dieser Gruppe erhalten über zusätzliche LDAP-ACLs die Berechtigung, Passwörter von anderen Benutzern zurückzusetzen. Diese LDAP-ACLs werden bei der Paketinstallation automatisch aktiviert. Um eine andere schon existierende Gruppe statt der Gruppe `User Password Admins` zu verwenden, kann der DN der zu verwendenden Gruppe in die Univention Configuration Registry Variable *ldap/acl/user/passwordreset/accesslist/groups/dn* (Seite 308) eingetragen werden. Nach der Änderung ist ein Neustart des LDAP-Servers erforderlich.

Passwörter können über das UMC-Modul *Benutzer* zurückgesetzt werden. In der Standardeinstellung wird das Modul nur dem Benutzer `Administrator` angezeigt. Während der Installation wird automatisch eine neue Richtlinie `default-user-password-admins` erstellt, die den Mitgliedern der Gruppe `User Password Admins` zugewiesen ist und mit einem entsprechenden Container im LDAP-Verzeichnis verknüpft werden kann. Weitere Hinweise zur Konfiguration von UMC-Richtlinien finden sich in Kapitel *Delegierte Administration für UMC-Module* (Seite 84).

Die Richtlinie ermöglicht dabei die Suche nach Benutzern sowie die Ansicht aller Attribute eines Benutzerobjektes. Wird versucht, neben dem Passwort weitere Attribute zu modifizieren, für die keine ausreichenden Zugriffsrechte auf das LDAP-Verzeichnis existieren, wird der Schreibzugriff vom Univention Directory Manager mit der Meldung *Zugriff verweigert* abgelehnt.

Vorsicht: Das Paket ist auf dem Primary Directory Node sowie den Backup Directory Nodes zu installieren. Während der Installation wird der LDAP-Server neu gestartet und ist kurzzeitig nicht erreichbar.

Das Zurücksetzen der Passwörter durch die Passwort-Gruppe kann für sensible Benutzer oder Gruppen (z.B. Domänen-Administratoren) verhindert werden. Mit den Univention Configuration Registry-Variablen *ldap/acl/user/passwordreset/protected/uid* (Seite 308) und *ldap/acl/user/passwordreset/protected/gid* (Seite 308) können Benutzer und Gruppen konfiguriert werden. Mehrere Werte müssen durch Kommas getrennt werden. Nach Änderungen an den Variable ist es erforderlich, den LDAP-Server über den Befehl **systemctl restart slapd** neu zu starten. In der Standardeinstellung werden die Mitglieder der Gruppe `Domain Admins` vor Passwortänderungen geschützt.

Sollte für die Änderung des Passworts der Zugriff auf zusätzliche LDAP-Attribute notwendig sein, können die Attributnamen in der Univention Configuration Registry Variable *ldap/acl/user/passwordreset/attributes* (Seite 308) ergänzt werden. Nach der Änderung ist zur Übernahme ein Neustart des LDAP-Verzeichnisdienstes notwendig. Für eine UCS-Standard-Installation ist diese Variable bereits passend gesetzt.

3.3.6 Name Service Switch / LDAP-NSS-Modul

Die in Univention Corporate Server verwendete GNU C-Standardbibliothek (**glibc**) bietet eine modulare Schnittstelle zur Auflösung von Namen von Benutzern, Gruppen und Rechnern, den *Name Service Switch*.

Das LDAP-NSS-Modul wird auf UCS-Systemen standardmäßig für den Zugriff auf die Domänen-Daten (z.B. Benutzer) verwendet. Das Modul greift dabei auf den in der Univention Configuration Registry Variable *ldap/server/name* (Seite 309) (und falls nötig zusätzlich der *ldap/server/addition* (Seite 309)) festgelegten LDAP-Server zu.

Das Verhalten bei nicht erreichbarem LDAP-Server kann durch die Univention Configuration Registry Variable *nssldap/bindpolicy* (Seite 314) festgelegt werden. Standardmäßig wird bei nicht erreichbarem Server eine erneute Verbindung aufgebaut. Wird die Variable auf `soft` gesetzt, wird kein erneuter Verbindungsaufbau durchgeführt. Dies kann den Boot eines Systems mit nicht erreichbarem LDAP-Server - z.B. in einer abgeschottenen Testumgebung - deutlich beschleunigen.

3.3.7 Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern

Für die Anbindung von nicht auf UCS-Systemen installierten OpenLDAP-Servern an das UCS-Managementsystem kann parallel zum Notifier-Dienst der Syncrepl-Replikationsdienst aktiviert werden. Dieser ist Bestandteil von OpenLDAP, registriert Veränderungen im lokalen Verzeichnisdienst und überträgt diese auf weitere OpenLDAP-Server.

3.3.8 Konfiguration des Verzeichnis-Dienstes bei Verwendung von Samba/AD

Standardmäßig ist der OpenLDAP-Server so konfiguriert, dass er zusätzlich zu den Standard-Ports `389` und `636` auch auf den Ports `7389` und `7636` Anfragen entgegen nimmt.

Wird Samba/AD eingesetzt, belegt der Dienst Samba/AD-Domänencontroller die Ports `389` und `636`. In diesem Fall wird OpenLDAP automatisch umkonfiguriert, so dass nur noch die Ports `7389` und `7636` eingesetzt werden. Dies ist insbesondere bei der Konfiguration von syncrepl zu beachten (siehe *Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern* (Seite 41)). **`univention-ldapsearch`** verwendet automatisch den Standard-Port.

3.3.9 Tägliche Sicherung der LDAP-Daten

Auf dem Primary Directory Node und allen Backup Directory Nodes wird der Inhalt des LDAP-Verzeichnisses durch einen Cron-Job täglich gesichert. Falls Samba 4 eingesetzt wird, werden auch dessen Daten-Verzeichnis gesichert.

Die LDAP-Daten werden im LDIF-Format im Verzeichnis `/var/univention-backup/` im Namensschema `ldap-backup_DATUM.ldif.gz` gespeichert. Sie sind nur für den Benutzer `root` lesbar. Die Samba 4 Backup-Dateien werden im Verzeichnis `/var/univention-backup/samba/` gesichert.

Mit der Univention Configuration Registry Variable *`backup/clean/max_age`* (Seite 303) kann definiert werden, wie lange alte Backup-Dateien aufgehoben werden (z.B. *`backup/clean/max_age`* (Seite 303)=`365`, alle Dateien älter als `365` Tage werden automatisch gelöscht). Diese Variable wird bei Neuinstallationen ab UCS 4.4-7 automatisch auf `365` gesetzt. Falls die Variable nicht gesetzt ist, werden keine Backup-Dateien gelöscht.

3.4 Listener/Notifier-Domänenreplikation

3.4.1 Ablauf der Listener/Notifier-Replikation

Die Replikation der Verzeichnisdaten innerhalb einer UCS-Domäne erfolgt über den Univention Directory Listener/Notifier-Mechanismus:

- Der Univention Directory Listener-Dienst läuft auf jedem UCS-System.
- Auf dem Primary Directory Node (und eventuell vorhandenen Backup Directory Nodes) überwacht der Univention Directory Notifier-Dienst Änderungen im LDAP-Verzeichnis und stellt die aufgezeichneten Änderungen transaktionsbasiert den Univention Directory Listener-Diensten auf den weiteren UCS-Systemen zur Verfügung.

Die aktiven Univention Directory Listener-Instanzen der Domäne verbinden sich zu einem Univention Directory Notifier-Dienst. Wird auf dem Primary Directory Node eine LDAP-Änderung durchgeführt (alle anderen LDAP-Server der Domäne sind nur lesend), wird diese durch den Univention Directory Notifier registriert und an die Listener-Instanzen gemeldet.

Jede Univention Directory Listener-Instanz verwendet eine Reihe von Univention Directory Listener-Modulen. Diese Module werden von den installierten Applikationen mitgeliefert, das Druckserver-Paket bringt z.B Listener-Module mit, die die CUPS-Konfiguration erzeugen.

Durch Univention Directory Listener-Module können Änderungen an der Domäne auch an Dienste übermittelt werden, die selbst nicht LDAP-fähig sind. Ein Beispiel ist der Druckserver CUPS: Die Druckerdefinitionen werden nicht aus dem LDAP ausgelesen, sondern aus der Datei `/etc/cups/printers.conf`. Wird nun im UMC-Modul

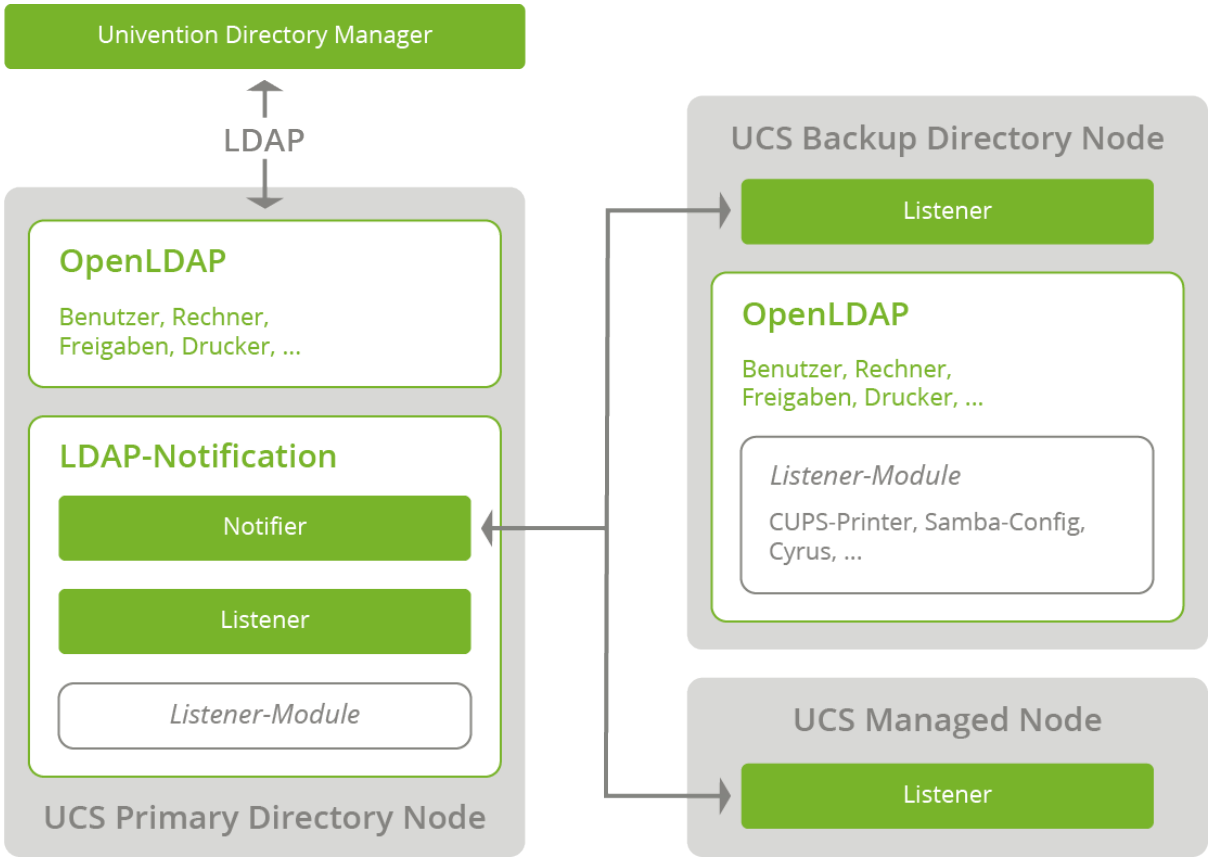


Abb. 3.2: Listener/Notifier-Mechanismus

Drucker ein Drucker angelegt, wird dieser im LDAP registriert. Diese Änderung wird dann vom Univention Directory Listener-Modul *cups-printers* erkannt und basierend auf den Daten im LDAP ein Eintrag in `/etc/cups/printers.conf` hinzugefügt, modifiziert oder gelöscht.

Weitergehende Informationen zum Aufbau von Univention Directory Listener-Modulen und zur Entwicklung eigener Module finden sich in *Univention Developer Reference* [3].

Die LDAP-Replikation erfolgt ebenfalls durch ein Listener-Modul. Ist der LDAP-Server zu dem repliziert werden soll nicht erreichbar, werden die LDAP-Änderungen in der Datei `/var/lib/univention-directory-replication/failed.ldif` zwischengespeichert. Der Inhalt dieser Datei wird beim späteren Start des LDAP-Servers automatisch in das LDAP übertragen.

Der Listener/Notifier-Mechanismus arbeitet transaktionsbasiert. Für jede Änderung im LDAP-Verzeichnis des Primary Directory Node wird eine Transaktions-ID erhöht. Eine Univention Directory Listener-Instanz, die mehrere Transaktionen verpasst hat - weil zum Beispiel der Rechner ausgeschaltet war - fragt bei erneuter Verfügbarkeit der Verbindung automatisch alle fehlenden Transaktionen ab, bis seine lokale Transaktions-ID der des Primary Directory Node entspricht.

3.4.2 Analyse von Listener/Notifier-Problemen

Logdateien/Debug-Level der Replikation

Alle Statusmeldungen des Univention Directory Listener und der aufgerufenen Listener-Module werden in die Datei `/var/log/univention/listener.log` protokolliert. Der Detailgrad der Logmeldungen kann über die Univention Configuration Registry Variable *listener/debug/level* (Seite 309) konfiguriert werden.

Statusmeldungen des Univention Directory Notifier-Dienstes werden in die Datei `/var/log/univention/notifier.log` protokolliert. Der Debuglevel kann mit der Variable *notifier/debug/level* (Seite 313) konfiguriert werden.

Erkennung von Replikationsproblemen

Im Regelbetrieb der Domänenreplikation (keine hohe Last auf den Systemen, keine Störungen im Netzwerk) ist die Verzögerung zwischen Änderungen in UMC-Modulen bis zur Replikation auf z.B. eines Replica Directory Node kaum merkbar. Eine möglicherweise unvollständige Replikation kann durch einen Vergleich der Transaktions-IDs von Listener- und Notifier-Dienst identifiziert werden.

Auf dem Primary Directory Node werden die vom Notifier-Dienst registrierten Transaktionen in aufsteigender Reihenfolge in die Datei `/var/lib/univention-ldap/notify/transaction` geschrieben. Ein Beispiel:

```
root@primary:~# tail -1 /var/lib/univention-ldap/notify/transaction
836 cn=replica3,cn=dc,cn=computers,dc=firma,dc=de m
```

Auf dem Listener-System wird die zuletzt vom Listener empfangene Transaktion in der Datei `/var/lib/univention-directory-listener/notifier_id` gespeichert:

```
root@replica1:~# cat /var/lib/univention-directory-listener/notifier_id
836
```

Diese Prüfung kann auch automatisiert durch den Nagios-Dienst `UNIVENTION_REPLICATION` durchgeführt werden (siehe *Vorkonfigurierte Nagios-Prüfungen* (Seite 300)).

Neuinitialiisierung von Listener-Modulen

Falls es zu Problemen bei der Abarbeitung eines Listener-Moduls gekommen ist, besteht die Möglichkeit, das Modul neu zu initialisieren. Dabei werden alle LDAP-Objekte mit denen das Listener-Modul arbeitet erneut übergeben.

> **Warnung:** Dies ist eine destruktive Operation. Sie entfernt internen Zustand des Listeners. Nur mit Vorsicht verwenden!

Dem Befehl zum erneuten Initialisieren muss der Name des Listener-Moduls übergeben werden. Die installierten Listener-Module sind im Verzeichnis `/var/lib/univention-directory-listener/handlers/` zu finden.

Mit dem folgenden Befehl kann beispielsweise das Druckermodul neu initialisiert werden:

```
$ univention-directory-listener-ctrl resync cups-printers
```

3.5 SSL-Zertifikatsverwaltung

Unter UCS werden sensitive Daten immer verschlüsselt über das Netzwerk übertragen, zum Beispiel durch die Verwendung von SSH für den Login auf Systeme oder durch Verwendung von Protokollen auf Basis von SSL/TLS. (*Transport Layer Security (TLS)* ist der aktuelle Protokollname, der Name des Vorgängerprotokolls *Secure Socket Layer (SSL)* ist jedoch weiterhin gebräuchlicher und wird auch in dieser Dokumentation verwendet).

SSL/TLS kommt beispielsweise bei der Listener/Notifier-Domänenreplikation oder beim HTTPS-Zugriff auf UCS Web-Oberflächen zum Einsatz.

Für eine verschlüsselte Kommunikation zwischen zwei Rechnern müssen beide Kommunikationspartner die Authentizität des verwendeten Schlüssels prüfen können. Dafür besitzt jeder Rechner ein so genanntes *Rechnerzertifikat*, das von einer Zertifizierungsstelle (Certification Authority, CA) herausgegeben und signiert wird.

UCS bringt seine eigene CA mit, die bei der Installation des Primary Directory Node automatisch eingerichtet wird und von der jedes UCS-System im Rahmen des Domänenbeitritts automatisch ein Zertifikat für sich selbst und das öffentliche Zertifikat der CA bezieht. Diese CA tritt als Root-CA auf, signiert ihr eigenes Zertifikat, und kann Zertifikate für andere Zertifizierungsstellen signieren.

Die Eigenschaften der CA werden bei der Installation basierend auf Systemeinstellungen wie der Locale automatisch festgelegt. Diese Einstellungen können auf dem Primary Directory Node im UMC-Modul *Zertifikats-Einstellungen* nachträglich angepasst werden.

Vorsicht: Besteht die UCS-Domäne aus mehr als einem System, müssen durch die Änderung des Root-Zertifikats auch alle anderen Rechner-Zertifikate neu ausgestellt werden! Das dafür nötige Vorgehen ist in KB 37 - Renewing the SSL certificates[8] dokumentiert.

Die UCS-CA befindet sich immer auf dem Primary Directory Node. Auf jedem Backup Directory Node wird eine Kopie der CA vorgehalten, die über einen Cronjob standardmäßig alle 20 Minuten mit der CA auf dem Primary Directory Node synchronisiert wird.

Vorsicht: Die CA wird nur vom Primary Directory Node zum Backup Directory Node synchronisiert und nicht umgekehrt. Es sollte also ausschließlich die CA auf dem Primary Directory Node verwendet werden.

Wird ein Backup Directory Node zum Primary Directory Node hochgestuft (siehe *Umwandlung eines Backup Directory Node zum neuen Primary Directory Node* (Seite 52)), so kann die CA auf dem dann neuen Primary Directory Node direkt verwendet werden.

Das UCS-Root-Zertifikat hat - ebenso wie die damit erstellten Rechnerzertifikate - einen bestimmten Gültigkeitszeitraum.

Vorsicht: Ist dieser Zeitraum abgelaufen, funktionieren Dienste, die ihre Kommunikation mit SSL verschlüsseln (z.B. LDAP oder die Domänenreplikation) nicht mehr.

Es ist deshalb notwendig, die Gültigkeit der Zertifikate regelmäßig zu überprüfen und rechtzeitig das Root-Zertifikat zu erneuern. Für die Überwachung des Gültigkeitszeitraums wird ein Nagios-Plugin bereitgestellt. Außerdem erfolgt beim Öffnen eines UMC-Moduls eine Warnmeldung, wenn das Root-Zertifikat bald abläuft (der Warnzeitraum kann mit der Univention Configuration Registry Variable `ssl/validity/warning` (Seite 318) festgelegt werden und beträgt standardmäßig 30 Tage).

Die Erneuerung des Root-Zertifikats und der übrigen Rechnerzertifikate ist in KB 37 - Renewing the SSL certificates[9] dokumentiert.

[8] https://help.univention.com/t/37
[9] https://help.univention.com/t/37

Auf UCS-Systemen überprüft ein Cronjob täglich die Gültigkeit des lokalen Rechnerzertifikats und des Root-Zertifikats und schreibt das Ablaufdatum in die Univention Configuration Registry-Variablen `ssl/validity/host` (Seite 318) (Rechnerzertifikat) und `ssl/validity/root` (Seite 318) (Root-Zertifikat). Die dort angegebenen Werte spiegeln die Anzahl der Tage seit dem 1.1.1970 wieder.

In Univention Management Console wird das effektive Ablaufdatum des Rechner- und Root-Zertifikats angezeigt über über das rechte, obere Benutzermenü und den Menüpunkt *Lizenz ▸ Lizenzinformation*.

3.6 Kerberos

Kerberos ist ein Authentifikationsverfahren um in verteilten Netzen über potentiell unsichere Verbindungen eine sichere Identifikation zu erlauben. Alle Clients verwenden dabei eine gemeinsame Vertrauensbasis, das *Key Distribution Centre* (KDC). Ein Client authentifiziert sich bei diesem KDC und erhält ein Authentifizierungstoken, das sogenannte Ticket, das zur Authentizierung innerhalb einer Kerberos-Umgebung (der sogenannten Kerberos Realm) verwendet werden kann. Der Name der Kerberos Realm wird im Rahmen der Installation des Primary Directory Node konfiguriert und in der Univention Configuration Registry Variable `kerberos/realm` (Seite 308) gespeichert. Der Name der Kerberos-Realm kann nachträglich nicht angepasst werden.

Tickets sind standardmäßig acht Stunden gültig; für eine Kerberos-Domäne ist deshalb eine synchrone Systemzeit zwischen den Systemen der Kerberos Realm essentiell.

In Univention Corporate Server wird die Kerberos-Implementierung Heimdal verwendet. Auf UCS Directory Nodes ohne Samba/AD wird ein eigenständiger Heimdal-Dienst gestartet, während auf Samba/AD-DCs Kerberos durch eine in Samba integrierte Heimdal-Version bereitgestellt wird. Verwendet man eine gemischte Umgebung aus UCS Directory Nodes mit Samba/AD und UCS Directory Nodes ohne Samba/AD, so basieren beide Kerberos-Umgebungen auf identischen Daten (diese werden zwischen Samba/AD und OpenLDAP durch den Univention S4 Connector synchronisiert (siehe *Univention S4 Connector* (Seite 179))).

3.6.1 KDC Auswahl

Standardmäßig wird der KDC über einen DNS-Servicerecord ausgewählt. Der von einem System verwendete KDC kann durch die Univention Configuration Registry Variable `kerberos/kdc` (Seite 307) umkonfiguriert werden. Wird Samba/AD auf einem System der Domäne installiert, wird der Servicerecord umkonfiguriert, so dass nur noch die KDCs auf Samba/AD-Basis angeboten werden. In einer gemischten Umgebung ist es empfehlenswert nur noch die Samba/AD-KDCs zu verwenden.

3.6.2 Kerberos Adminserver

Auf dem Primary Directory Node läuft der Kerberos-Adminserver, auf dem administrative Einstellungen der Domäne vorgenommen werden können. Die meisten Einstellungen werden in Univention Corporate Server aus dem LDAP-Verzeichnis bezogen, so dass die wichtigste verbleibende Funktion das Ändern von Passwörtern darstellt. Diese können durch das Tool **kpasswd** geändert werden und werden dann auch im LDAP verändert. Der Kerberos Adminserver kann auf einem System durch die Univention Configuration Registry Variable `kerberos/adminserver` (Seite 307) konfiguriert werden.

3.7 Passwort-Hashes im Verzeichnisdienst

Passwort-Hashes von Benutzern werden u.a. im Attribut `userPassword` im Verzeichnisdienst gespeichert. Für die Generierung der Passwort-Hashes wird auf die **`crypt`** Bibliotheksfunktion zurückgegriffen. Die eigentliche Hash-Funktion kann über die Univention Configuration Registry Variable *`password/hashing/method`* (Seite 315) definiert werden, standardmäßig wird `SHA-512` verwendet.

Alternativ dazu bietet Univention Corporate Server ab UCS 4.4 erratum 887[10] die Möglichkeit **`bcrypt`** als Hash-Funktion für Benutzerkonten zu verwenden. Dafür muss zunächst auf allen LDAP-Servern die Univention Configuration Registry Variable *`ldap/pw-bcrypt`* (Seite 309) auf `true` gesetzt werden um das nötige Modul für OpenLDAP zu aktivieren. Andernfalls ist eine Anmeldung am LDAP-Server mit einem **`bcrypt`** Hash nicht möglich. Damit beim Ändern von Passwörtern nun **`bcrypt`** Hashes generiert werden, muss ebenfalls auf allen Servern die Univention Configuration Registry Variable *`password/hashing/bcrypt`* (Seite 314) auf `true` gesetzt werden.

Zusätzlich können der *bcrypt Cost Factor* und die **`bcrypt`** Variante über die Univention Configuration Registry Variablen *`password/hashing/bcrypt/cost_factor`* (Seite 315) (`12`) und *`password/hashing/bcrypt/prefix`* (Seite 315) (`2b`) angepasst werden.

Vorsicht: **`bcrypt`** ist auf maximal 72 Zeichen begrenzt. Für die Generierung der Hashes werden also nur die ersten 72 Zeichen des Passwortes verwendet.

3.8 SAML Identity Provider

SAML (Security Assertion Markup Language) ist ein XML-basierter Standard zum Austausch von Authentifizierungsinformationen, der *Single Sign-On* über Domänengrenzen hinweg erlaubt. UCS stellt auf dem Primary Directory Node und den Backup Directory Node einen ausfallsicheren SAML Identity Provider bereit. Über ein kryptografisches Zertifikat wird der SAML Identity Provider bei einem externen Dienst fest registriert und vertraut diesem. Der Benutzer authentifiziert sich dann einmalig gegenüber UCS und kann den Dienst ohne erneute Authentifizierung nutzen.

Der SAML 2.0 kompatible UCS Identity Provider wird durch die Integration von **`simplesamlphp`** bereitgestellt.

Der UCS Identity Provider ist eng in die UCS Domäne eingebunden. Daher müssen Rechner, von denen der UCS Identity Provider genutzt werden soll, DNS-Namen in der UCS-Domäne auflösen können. Die DNS-Server der Domäne sollten auf allen Clients eingetragen sein, um den zentralen DNS-Namen, im Normalfall `ucs-sso.`*`[domainname]`*, auflösen zu können.

Der UCS Identity Provider wird auf dem Primary Directory Node und Backup Directory Node mit der Installation automatisch eingerichtet. Um die Ausfallsicherheit innerhalb der Domäne zu erhöhen, können weitere Systeme der Rolle Backup Directory Node verfügbar gemacht werden. Für den ausfallsicheren Zugriff auf den UCS Identity Provider wird standardmäßig der DNS-Eintrag `ucs-sso.`*`[domainname]`* registriert. Das für diesen Eintrag vorgesehene TLS Zertifikat wird auf allen beteiligten Systemen der Domäne vorgehalten. Es wird empfohlen, das Wurzelzertifikat der UCS Domäne auf allen Rechnern, die *Single Sign-On* nutzen, zu installieren.

Es besteht die Möglichkeit, die SAML-Authentifizierung mit der Kerberos Anmeldung zu verknüpfen. Das bedeutet, dass sich Nutzer mit einem gültigen Kerberos Ticket, z.B. nach einer Anmeldung an Windows oder Linux, ohne eine erneute manuelle Authentifizierung am Identity Provider anmelden können.

Um die Kerberos Authentifizierung am Identity Provider zuzulassen, muss die Univention Configuration Registry Variable *`saml/idp/authsource`* (Seite 317) von `univention-ldap` auf `univention-negotiate` gesetzt werden. Die Webbrowser müssen entsprechend so konfiguriert werden, so dass das Kerberos Ticket an den SAML Identity Provider übertragen wird. Im folgenden beispielhaft für Firefox und den Internet Explorer / Microsoft Edge:

Mozilla Firefox

In der erweiterten Firefox Konfiguration, diese ist erreichbar über die Eingabe von `about:config` in der

[10] https://errata.software-univention.de/#/?erratum=4.4x887

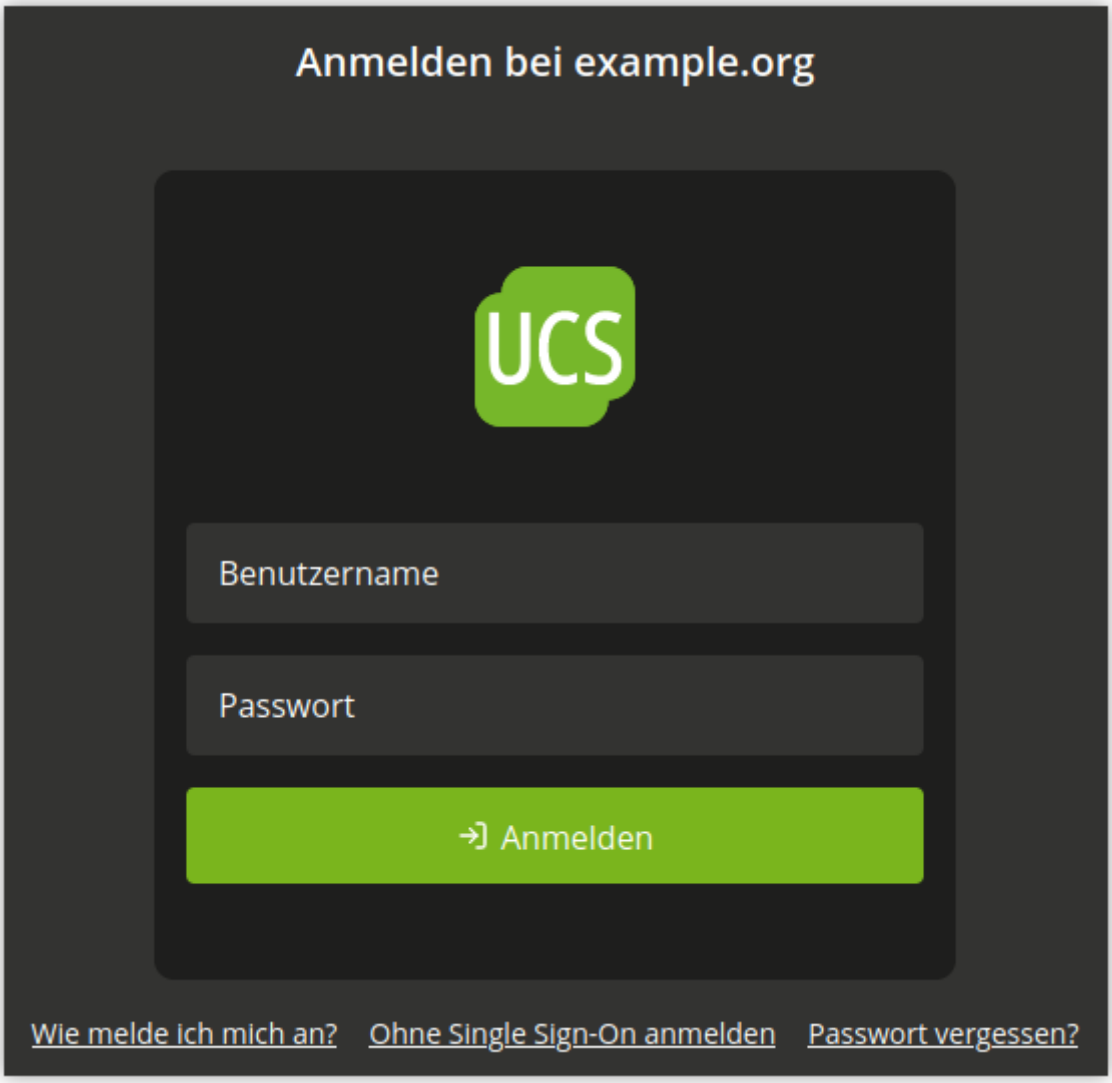


Abb. 3.3: Die Single Sign-On Anmeldeseite

Firefox Adresszeile, muss bei der Option `network.negotiate-auth.trusted-uris` die Adresse des Identity Providers eingetragen werden, also in der Standardeinstellung `ucs-sso.[domainname]`.

Microsoft Internet Explorer; Microsoft Edge
In der Systemsteuerung müssen die *Internetoptionen* geöffnet werden und dort wird unter *Sicherheit* ‣ *Lokales Intranet* ‣ *Sites* ‣ *Erweitert* die Adresse des Identity Providers hinzugefügt, also in der Standardeinstellung `ucs-sso.[domainname]`.

Die Kerberos Authentifizierung kann auf bestimmte IP Subnetze beschränkt werden, indem die Univention Configuration Registry Variable *saml/idp/negotiate/filter-subnets* (Seite 317) beispielsweise auf `127.0.0.0/16,192.168.0.0/16` gesetzt wird. Dies ist besonders nützlich, um zu verhindern, dass für Clients, die nicht zur UCS-Domäne gehören, ein Dialog für den Login angezeigt wird.

3.8.1 Anmelden per Single Sign-On

Die Aktivierung von *Single Sign-On* für das Portal wird in *Anmelden* (Seite 60) beschrieben. Dafür muss `ucs-sso.[Domain name]` erreichbar sein. Anmeldedaten des Domänenkontos verwendet. Für den Login direkt am UCS-System (also ohne *Single Sign-On*) gelangt man über den Link *Ohne Single Sign-On anmelden*.

Über die Datei `/usr/share/univention-management-console-login/css/custom.css` kann das Design des Anmeldedialogs angepasst werden. Diese Datei wird niemals automatisch überschrieben.

Andere Webdienste leiten ebenfalls auf die Anmeldeseite des UCS Identity Providers weiter, wenn ein *Single Sign-On* durchgeführt wird. Nach erfolgreicher Authentifizierung wird der Benutzer wieder auf die Seite des Webdienstes gesendet werden. Diese Dienste müssen, wie in *Hinzufügen eines neuen externen Service Providers* (Seite 48) beschrieben, registriert werden.

Der *Single Sign-On* an einem Dienst kann auch vom UCS Identity Provider initiiert werden. Dies erspart den Umweg, zunächst den externen Dienst selbst aufzurufen und sich von dort zur Authentifizierung weiterleiten zu lassen. Dazu muss der Identity Provider mit einem Link der Form `https://ucs-sso.[domainname]/simplesamlphp/saml2/idp/SSOService.php?spentityid=[Service provider identifier]` aufgerufen werden.

3.8.2 Hinzufügen eines neuen externen Service Providers

Die am UCS Identity Provider registrierten Service Provider können über das UMC-Modul *SAML Identity Provider* verwaltet werden. Benutzer müssen freigeschaltet werden, bevor sie sich am UCS Identity Provider für einen Dienst authentifizieren können. Service Provider können auch für Gruppen aktiviert werden, sodass sich alle Benutzer in dieser Gruppe für diesen Dienst authentifizieren können. Auf dem Reiter *Konto* eines Benutzers, oder dem Reiter *Allgemein* einer Gruppe, muss dazu unter *SAML Einstellungen* der Service Provider Eintrag hinzugefügt werden.

Um den UCS Identity Provider bei einem SAML Service Provider zu registrieren, wird der öffentliche Teil des SAML-Zertifikats auf dem Service Provider benötigt. Dieses kann über einen Download-Link im UMC-Modul heruntergeladen werden. Andere Service Provider benötigen die XML-Metadaten des Identity Providers in Form eines Datei-*Uploads*. In der Standardkonfiguration kann die XML-Datei unter der URL `https://ucs-sso.[domainname]/simplesamlphp/saml2/idp/metadata.php` heruntergeladen werden.

Die folgenden Attribute können beim Anlegen eines neuen Service Provider-Eintrags konfiguriert werden.

Tab. 3.1: Allgemeine Felder bei der Anbindung eines Service Providers

Attribut	Beschreibung
Service Provider aktivieren	Ist diese Option gesetzt, wird die Konfiguration des Service Providers aktiviert und steht für die Anmeldung bereit.
Bezeichner des Service Providers	Definiert den internen Namen des Service Providers. Dieser wird später am Benutzerobjekt angezeigt und ausgewählt, um Benutzer für die Verbindung freizuschalten. Der Bezeichner kann später nicht mehr geändert werden.
Antwort an diese Service Provider URL nach dem Login	Nach dem erfolgreichen Login an UCS wird der Browser des Benutzers zurück zum Service Provider geleitet. Die Weiterleitung erfolgt an die hier angegebene URL.
Single Logout URL des Service Providers	Service Provider können einen URL Endpunkt anbieten, mit dem die Session am Service Provider beendet werden kann. Loggt sich der Benutzer am UCS Identity Provider aus, wird über die hier übergebene URL eine Abmeldung am Service Provider durchgeführt.
Format des `NameID` Attributs	Der Wert `NameIDFormat`, den der Service Provider erhält. Die Dokumentation des Service Providers sollte erwartete Formate erwähnen. Beispiel: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` oder `urn:oasis:names:tc :SAML:1.1:nameid-format:unspecified`.
Name des Attributs, das als `NameID` verwendet wird	Hier kann das LDAP Attribut eingetragen werden, das für eine eindeutige Identifizierung des Benutzers am Service Provider verwendet wird, beispielsweise `uid`.
Name der Organisation des Service Providers	Der hier eingetragene Wert wird auf der UCS Single Sign-On Anmeldeseite angezeigt. Dem Benutzer wird so dargestellt, für welchen Dienst er sich authentifiziert.
Beschreibung dieses Service Providers	Der hier eingetragene Wert wird auf der UCS Single Sign-On Anmeldeseite angezeigt. Hier kann eine längere Beschreibung über den Dienst angegeben werden, der auf der Login Seite in einem eigenen Absatz angezeigt wird.

Tab. 3.2: Erweiterte Felder bei der Anbindung eines Service Providers

Attribut	Beschreibung
URL zur Datenschutzrichtlinie des Service Providers	Wird hier eine URL eingetragen, wird dem Benutzer ein Link zu dieser Seite auf der UCS Identity Provider-Login-Seite angezeigt.
Erlaube die Übertragung von LDAP Attributen an den Service Provider	Standardmäßig überträgt der UCS Identity Provider nur das auf dem Reiter *Allgemein* angegebene `NameID` Attribut an den Service Provider. Benötigt der Service Provider weitere LDAP-Benutzerattribute, kann diese Checkbox aktiviert werden. Die zu übertragenen Attribute werden dann unter *Liste der zu übermittelnden LDAP Attribute* eingetragen.
Der Wert des `attribute format` Feldes	Sollen die übertragenen Attribute mit einem besonderen Format übertragen werden, kann dieser hier eingetragen werden. Beispiel: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` oder `urn:oasis:names:tc :SAML:1.1:nameid-format:unspecified`.
Liste der zu übermittelnden LDAP-Attribute	Hier kann jedes zu übertragende LDAP-Attribut eingetragen werden. Zu jedem dieser Attribute können ebenfalls ein oder mehrere Service Attribut-Namen im nebenstehenden Feld definiert werden. Diese dienen zur Übersetzung des LDAP Attribut-Namen für den Service-Provider. Mehrere Einträge müssen durch Kommata getrennt werden. Damit der UCS Identity Provider die angegebenen Attribute verarbeiten kann, müssen sie zusätzlich am LDAP Objekt `id=default-saml-idp, cn=univention,` *`[base DN]`* eingetragen werden. Dort eingetragene LDAP Attribute können vom Identity Provider ausgelesen und übertragen werden.

3.8.3 Erweiterte Konfiguration

In manchen Umgebungen kann es erforderlich sein, dass der UCS Identity Provider mehrere logische Identity Provider Instanzen bereitstellt. Die logische Trennung wird erreicht, indem der Identity Provider unterschiedliche URIs als Endpunkt anbietet.

Der standardmäßig eingerichtete Endpunkt ist `https://ucs-sso.[domainname]/simplesamlphp/saml2/idp/metadata.php`. Weitere Einträge können durch das Setzen von Univention Configuration Registry Variablen in der Form *saml/idp/entityID/supplement/[identifier]* (Seite 317) auf `true` erzeugt werden. Diese müssen auf allen Servern, die den UCS Identity Provider zur Verfügung stellen, gesetzt werden. Typischerweise sind dies der Primary Directory Node und alle Server der Rolle Backup Directory Node. Anschließend muss der **apache2** Dienst neu geladen werden.

Um beispielsweise einen weiteren Eintrag unter der URI `https://ucs-sso.[domainname]/simplesamlphp/[secondIDP]/saml2/idp/metadata.php` einzurichten, muss die Univention Configuration Registry Variable `saml/idp/entityID/supplement/secondIDP=true` gesetzt werden.

3.9 OpenID Connect Provider

UCS bietet die Möglichkeit, einen *OpenID Connect Provider* zu installieren, mit dessen Hilfe externe Web-Dienste die Benutzeranmeldung über das *OpenID Connect (OIDC)* Protokoll an das UCS Identity Management delegieren können. Die **OpenID Connect Provider** App kann über das App Center installiert werden. Der Dienst wird von der Software **Kopano Konnect** bereitgestellt.

Die App kann grundsätzlich auf allen Systemrollen installiert werden. Bei einer Installation auf einem UCS System der Rolle Primary Directory Node oder Backup Directory Node wird der **OpenID Connect Provider** unter dem DNS Eintrag für den *Single Sign-On* verfügbar gemacht, im Normalfall ist dies `ucs-sso.domain.name`.

Wird die App auf einer anderen Systemrolle installiert, kann der Provider statt dessen direkt über den Hostnamen erreicht werden. Es sollte sichergestellt werden, dass die App auf allen Servern installiert ist, die unter dem `ucs-sso` DNS CNAME erreichbar sind.

Die Synchronisation von Session Informationen zwischen mehreren Instanzen des OIDC Providers ist nicht vorkonfiguriert. Wenn Login Probleme bei Apps in dieser Konfiguration auftreten, empfehlen wir den OIDC Provider nur auf einem System zu betreiben, und den `ucs-sso` DNS CNAME auf dieses System zu beschränken, oder den Univention Support zu kontaktieren.

Um externe Web-Dienste per **OpenID Connect** an UCS anzubinden, muss für diesen Dienst ein bestimmtes Objekt des Typs `oidc/rpservice` im UCS Verzeichnisdienst vorhanden sein. Dies kann im UMC-Modul *LDAP-Verzeichnis* im Container `cn=oidc` angelegt werden, der sich unterhalb des Containers `cn=univention` befindet. Hier kann über die Schaltfläche *Hinzufügen* und die Auswahl *OpenID Connect Relying Party Service* ein neuer Dienst registriert werden.

Das gleiche ist auch über die Kommandozeile möglich:

```
$ udm oidc/rpservice create --set name=$UCS_interner_Bezeichner> \
  --position="cn=oidc,cn=univention,$(ucr get ldap/base)" \
  --set clientid="$ClientID" \
  --set clientsecret="$ein_langes_Passwort" \
  --set trusted=yes \
  --set applicationtype=web \
  --set redirectURI="$URL_aus_der_Dokumentation_des_Dienstes"
```

Die Parameter des Aufrufs sind:

name
: der beim Login im Webinterface angezeigte Dienstname.

clientid
: müssen hier und beim angebundenen Dienst identisch sein (*shared secret*).

secret
müssen hier und beim angebundenen Dienst identisch sein (*shared secret*).

trusted
sollte standardmäßig auf `yes` gesetzt werden. Andernfalls wird dem Benutzer eine Bitte um Bestätigung zur Übertragung seiner Benutzerattribute an den Dienst angezeigt.

applicationtype
sollte für Internetdienste auf den Wert `web` gesetzt werden.

redirectURI
URL des Login-Endpunkts, die in der Dokumentation des jeweiligen angebundenen Dienstes zu finden ist. Ist ein Dienst über mehrere URLs erreichbar oder soll er auch per IP Adresse aufrufbar sein, müssen alle möglichen Adressen zum Attribut `redirectURI` hinzugefügt werden. Das Feld kann daher mehrfach definiert werden, wobei jeder einzelne Wert eine gültige URL enthalten muss.

Der angebundene Web-Dienst braucht für seine Konfiguration noch Informationen über die *OpenID Connect* Endpunkte der Provider-App. Diese sind bei installierter Provider-App unter der URL `https://ucs-sso.`*`[Domain Name]`*`/.well-known/openid-configuration` einsehbar. Wurde die Provider-App auf einem anderen System als Primary Directory Node oder Backup Directory Node installiert, ist wie oben beschrieben statt `ucs-sso.`*`Domain Name`* der FQDN des jeweiligen Servers zu verwenden.

Bei der Verwendung von *OpenID Connect* ist auf korrekte, auflösbare DNS Namen und verifizierbare Zertifikate zu achten. Zu beachten ist dies insbesondere bei Client-Rechnern von Endbenutzern, die sowohl auf die per DNS auflösbaren Hostnamen des Web-Dienst als auch auf den OpenID Connect Provider zugreifen müssen. Außerdem müssen die extern angebundenen Web-Dienste eine Verbindung zum OpenID Connect Provider herstellen können, um darüber die Benutzerattribute abrufen zu können.

Im speziellen Fall, wo der DNS Namen des OIDC-Providers geändert werden soll, muss zunächst der entsprechende Wert in den App Einstellungen der **OpenID Connect Provider** App angepasst werden. Da es diverse Szenarien für die Erreichbarkeit des Providers nach der Änderung des DNS Namens gibt, kann keine automatische Änderung der Webserverkonfiguration vorgenommen werden. Es muss so zum Beispiel je nach konfiguriertem DNS Namen noch die Apache Konfiguration unter UCS angepasst werden. Die Konfigurationsdatei `/etc/apache2/conf-available/openid-connect-provider.conf` muss unter dem gesetzten DNS Namen in einem Virtual Host verfügbar gemacht werden.

Mit Version 2 der OIDC-Provider App funktioniert die Authentifizierung an **OpenID Connect** über den SAML Identity Provider der UCS Domäne. Ist der SAML Identity Provider von der Standardkonfiguration abweichend nicht unter `https://ucs-sso.`*`[domain.name]`* erreichbar, muss in den App Einstellungen die URL korrekt eingetragen werden, unter der die SAML IdP Metadaten für die UCS Domäne abgerufen werden können. Bei inkorrekter Konfiguration dieser URL startet der OpenID Connect Provider nicht.

Mit der Authentifizierung per SAML ist die Autorisierung für die Nutzung des OpenID Connect Providers und damit zu allen per OIDC angebundenen Apps über SAML Berechtigungen steuerbar. Standardmäßig wird bei der Installation der App die Gruppe `Domänenbenutzer` für den Zugriff freigeschaltet. Wenn diese Berechtigung entfernt werden soll, muss zusätzlich in den App Einstellungen die entsprechende Option aktiviert werden, damit die Berechtigung nicht automatisch erneut hinzugefügt wird.

Der OpenID Connect Provider protokolliert Aktionen über den Docker Daemon. Die Ausgaben können beispielsweise über das Kommando **univention-app logs openid-connect-provider** eingesehen werden.

3.10 Umwandlung eines Backup Directory Node zum neuen Primary Directory Node

Eine UCS Domäne hat immer genau einen Primary Directory Node, kann aber beliebig viele Backup Directory Node beinhalten. Ein Backup Directory Node speichert alle Domänendaten und alle SSL-Sicherheitszertifikate als Kopie, im Gegensatz zum Primary Directory Node können jedoch keine schreibenden Änderungen vorgenommen werden.

Jeder Backup Directory Node kann zu einem Primary Directory Node umgewandelt werden. Hierfür gibt es zwei typische Anwendungsfälle:

- Im Notfall nach einem Hardwareausfall des Primary Directory Node.
- Zum geplanten Ersetzen des Primary Directory Node durch neue Hardware oder Wechsel der Architektur von *i386* auf *amd64*.

Vorsicht: Die Umwandlung eines Backup Directory Node in einen Primary Directory Node ist ein tiefgreifender Konfigurationsschritt und sollte gründlich vorbereitet werden! Die Umwandlung kann nicht rückgängig gemacht werden.

Der zu ersetzende Primary Directory Node muss vor Beginn der Umwandlung abgeschaltet werden und darf weder während der Umwandlung noch im Anschluss daran wieder in Betrieb genommen werden!

Im Vorfeld muss die installierte Software sowie die aktuelle Konfiguration zwischen Primary Directory Node und Backup Directory Node abgeglichen werden. Wenn der Primary Directory Node wegen eines Ausfalls nicht mehr verfügbar ist, muss eine Sicherung herangezogen werden. Im Nachgang an die Umwandlung müssen alle möglichen verbliebenen Referenzen auf den alten Primary Directory Node entfernt oder korrigiert werden.

Die Umwandlung umfasst primär die Umstellung der für die Authentifizierung relevanten Dienste wie LDAP, DNS, Kerberos und Samba. Der Abgleich der installierten Software muss manuell erfolgen (über die UMC-Module *App Center* und *Paket-Verwaltung*).

Wenn also z.B. auf dem vorherigen Primary Directory Node die Mailkomponente installiert war, ist diese nach der Umwandlung nicht automatisch auf dem neuen Primary Directory Node verfügbar. Um den Umfang der Nachbereitung möglichst gering zu halten, sollte im Vorfeld *Fehlertolerante Domain Einrichtung* (Seite 54) beachtet werden.

Wurden auf dem Primary Directory Node zusätzliche LDAP-Schema-Pakete installiert, so müssen diese vor der Umwandlung auch auf dem Backup Directory Node installiert werden. Die Paketliste des alten Primary Directory Node sollte vor der Umstellung gesichert werden, um einen Abgleich der installierten Pakete zu erlauben. Die Paketliste kann mit dem folgenden Befehl erstellt werden:

```
$ dpkg --get-selections \* > dpkg.selection
```

Vergleichen Sie die so auf dem Primary Directory Node erstellte Datei mit einer ebenso erstellten Datei des Backup Directory Node. Sie sollten sich lediglich in den Paketen **univention-server-master** und **univention-server-backup** unterscheiden. Installieren Sie die benötigten Pakete auf dem Backup Directory Node nach. Insbesondere alle Pakete, die ein LDAP-Schema installieren, sind zwingend erforderlich. Der folgende Befehl ausgeführt auf dem Primary Directory Node erstellt eine Auflistung aller Pakte mit LDAP-Schema:

```
$ dpkg -S /etc/ldap/schema/*.schema \
  /usr/share/univention-ldap/schema/*.schema
```

Um einfach alle installierten Pakete des Primary Directory Node auch auf dem Backup Directory Node zu installieren, kann die zuvor auf dem Primary Directory Node erstellte Datei `dpkg.selection` mit folgenden Befehlen verwendet werden:

```
$ dpkg --set-selections < dpkg.selection
$ apt-get dselect-upgrade
```

Darüber hinaus sollte der Univention Configuration Registry-Datenbestand gesichert werden, um Konfigurationsanpassungen auch auf dem neuen Primary Directory Node abgleichen zu können. Folgende Dateien des Primary

Directory Node sind dazu mit denen auf dem Backup Directory Node zu vergleichen:

- `/etc/univention/base.conf`
- `/etc/univention/base-forced.conf`

Eine nächtliche Sicherung dieser Dateien findet sich auch in `/var/univention-backup/ucr-backup_%Y%m%d.tgz`.

Die Umwandlung eines Backup Directory Node zum neuen Primary Directory Node erfolgt dann durch Aufruf des Befehls **`/usr/lib/univention-ldap/univention-backup2master`** auf dem Backup Directory Node. Das System muss anschließend neu gestartet werden. Die Umstellung wird in der Logdatei `/var/log/univention/backup2master.log` protokolliert. Folgende Schritte führt der Befehl **`univention-backup2master`** der Reihe nach aus:

1. Prüfung der Umgebung: Bei dem System muss es sich um einen Backup Directory Node handeln, der der Domäne bereits beigetreten ist. Zudem wird sichergestellt, dass der Primary Directory Node über DNS auflösbar sowie dass eine Verbindung zum Repository-Server möglich ist. Außerdem darf der Primary Directory Node nicht mehr im Netzwerk erreichbar sein.
2. Nun werden die wichtigsten Dienste OpenLDAP, Samba, Kerberos sowie Univention Directory Notifier und Listener gestoppt, elementare Univention Configuration Registry Variable wie *`ldap/master`* (Seite 309) und *`server/role`* (Seite 317) umgestellt, das UCS Root-Zertifikat vom Webserver des Backup Directory Node abrufbar gemacht und die oben genannten Dienste wieder gestartet.
3. Der DNS SRV Eintrag `kerberos-adm` wird vom alten auf den neuen Primary Directory Node geändert.
4. Sofern vorhanden, wird der Univention S4 Connector (siehe *Univention S4 Connector* (Seite 179)) vom Rechnerobjekt des alten Primary Directory Node entfernt und auf dem neuen Primary Directory Node zur erneuten Konfiguration vorgemerkt.
5. Im OpenLDAP wird die Serverrolle des neuen Primary Directory Node auf `domaincontroller_master` geändert. Ebenfalls wird der DNS SRV Eintrag `_domaincontroller_master._tcp` korrigiert.
6. Sofern vorhanden werden die Einträge des alten Primary Directory Node aus der lokalen Samba-Datenbank des neuen Primary Directory Node entfernt. Zudem werden die FSMO-Rollen auf den neuen Primary Directory Node übertragen.
7. Anschließend wird das Rechnerobjekt des alten Primary Directory Node im OpenLDAP gelöscht.
8. Nun wird das LDAP nach Referenzen auf den alten Primary Directory Node durchsucht. Alle gefundenen Referenzen werden angezeigt und es wird eine Korrektur vorgeschlagen, welche einzeln geprüft und bestätigt werden muss, z.B. weitere DNS-Einträge.
9. Zum Abschluss wird das Paket **`univention-server-backup`** durch **`univention-server-master`** ersetzt.

Im Anschluss sollte sowohl Univention Configuration Registry auf allen UCS-Systemen der Domäne als auch das LDAP auf dem jetzt neuen Primary Directory Node hinsichtlich Verweisen auf den Namen und die IP-Adresse des alten Primary Directory Node überprüft und diese angepasst werden.

Für weitere Hinweise, siehe Univention Help 19514 - „How To: backup2master“[11].

[11] https://help.univention.com/t/19514

3.11 Fehlertolerante Domain Einrichtung

Einige Dienste in einer Domäne sind zentral für das Funktionieren von deren Mitgliedern. Redundanz ist ein Mittel um diesen potenziellen Bruchstellen (*single points of failure*) zu entfernen. Ein Artikel in der Univention Support Datenbank erklärt das Vorgehen um die Dienste LDAP, Kerberos, DNS, DHCP und Active Directory-kompatible Domain Controller abzusichern: KB 6682 - Fail-safe domain setup[12].

3.12 Protokollierung von Aktivitäten in der Domäne

Über die **`Admin Diary`** App besteht die Möglichkeit, wichtige Ereignisse in der Domäne zu protokollieren. Dazu gehören unter anderem:

- Das Anlegen, Verschieben, Verändern oder Löschen von Benutzern und anderen Objekten über Univention Directory Manager
- Installation, Update und Deinstallation von Apps
- Server-Passwort-Änderungen
- Start, Ende und eventuelle Fehler bei Domänenbeitritten
- Start und Ende von UCS Updates

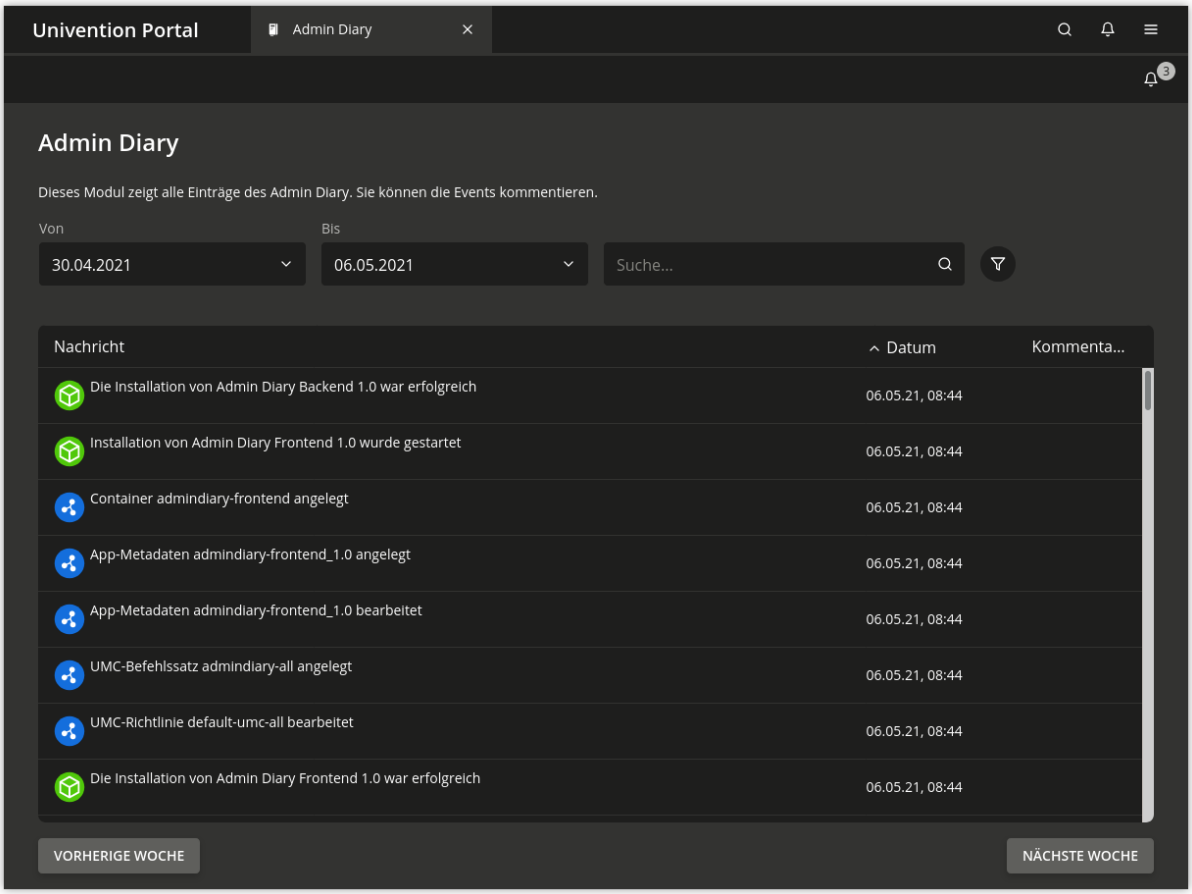


Abb. 3.4: Ansicht der Ereignisse im Admin Diary

Abb. 3.4 zeigt, wie die Ereignisse im UMC-Modul *Admin Diary* dargestellt werden. Die angezeigten Einträge werden standardmäßig wochenweise gruppiert und können über das Suchfeld weiter eingegrenzt werden. Durch das Auswäh-

[12] https://help.univention.com/t/6682

len eines Eintrags gelangt man zu einer Detailansicht, wie sie in Abb. 3.5 zu sehen ist. Dieser kann man weitere Details zum Wo und Wann entnehmen. Zudem besteht die Möglichkeit, das Ereignis zu kommentieren.

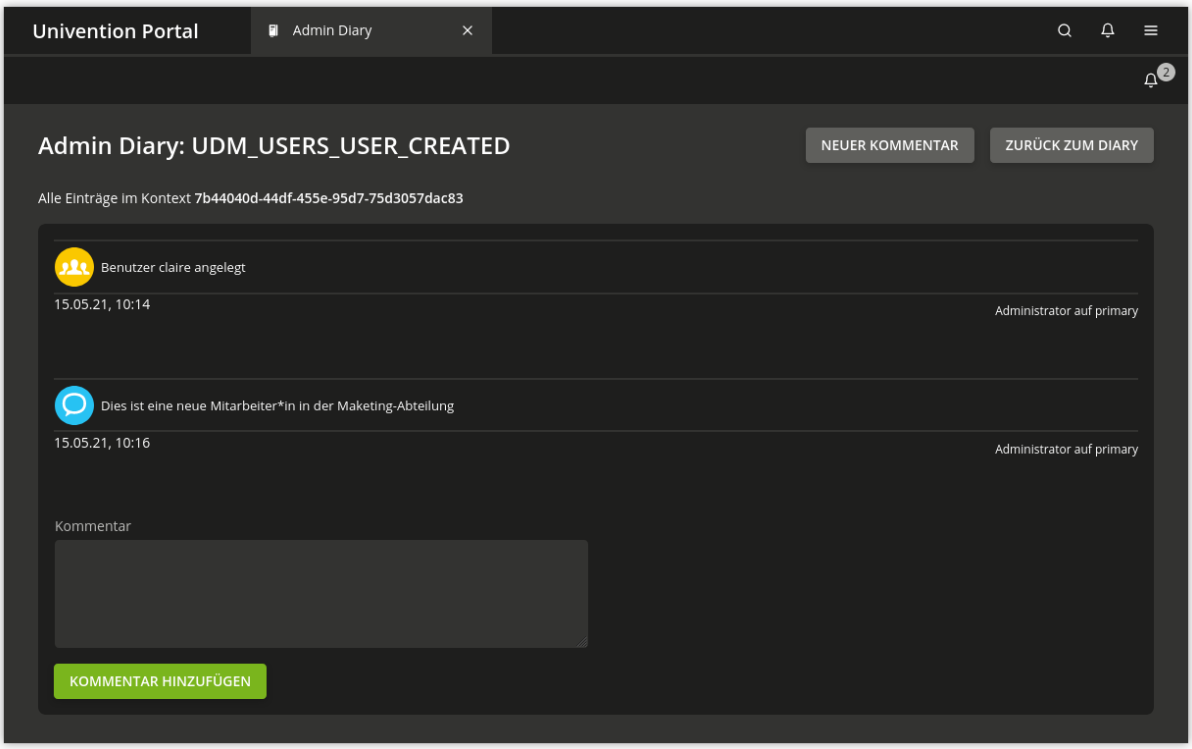


Abb. 3.5: Detailansicht im Admin Diary

Die App besteht aus zwei Komponenten:

Admin Diary Backend
: Das Backend muss auf einem System in der Domäne installiert sein, bevor das Frontend installiert werden kann. Es beinhaltet eine Anpassung für `rsyslog` und schreibt in eine zentrale Datenbank, standardmäßig PostgreSQL. Falls MariaDB oder MySQL vorher auf dem Zielsystem installiert ist, dann wird es statt PostgreSQL verwendet.

Admin Diary Frontend
: Auch das Frontend muss mindestens einmal installiert sein, kann aber öfter installiert werden. Das Frontend beinhaltet das UMC-Modul *Admin Diary*, um die Einträge anzuzeigen und zu kommentieren. Wenn es nicht auf dem selben System installiert werden soll, auf dem das Backend läuft, dann muss der Zugriff auf die zentrale Datenbank manuell eingerichtet werden. Die dazu notwendigen Schritte sind in Admin Diary - How to separate front end and back end[13] beschrieben.

[13] https://help.univention.com/t/admin-diary-how-to-seperate-frontend-and-backend/11331

KAPITEL 4

UCS Web-Oberfläche

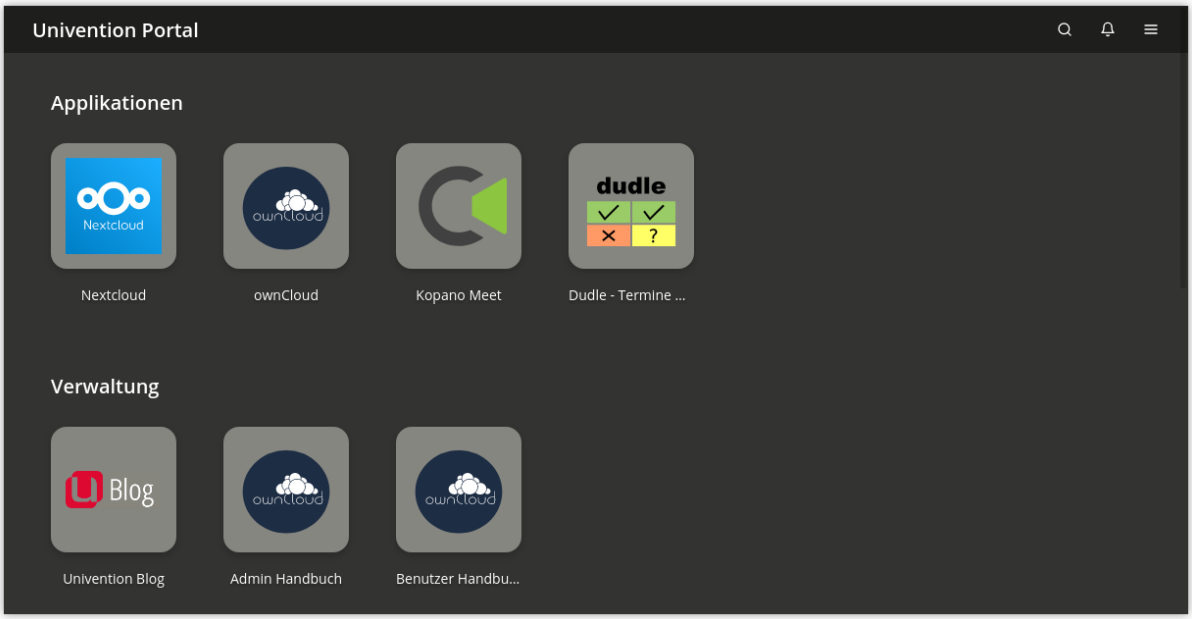


Abb. 4.1: UCS Portalseite

Die UCS Web-Oberfläche ist das zentrale Werkzeug zur Verwaltung der UCS-Domäne sowie für den Zugriff auf installierte Applikationen derselben.

Die UCS Web-Oberfläche untergliedert sich in mehrere Unterseiten, die alle eine ähnlich gestaltete Kopfzeile besitzen. Über die Symbole oben rechts kann eine Suche auf der aktuellen Seite durchgeführt (Lupe) oder das Benutzermenü (drei Balken) geöffnet werden (dort kann man sich auch anmelden). Die Anmeldung an der Oberfläche geschieht über eine zentrale Seite für alle Unterseiten von UCS sowie Drittherstellern, sofern diese einen webbasierten *Single Sign-on* unterstützen (*Anmelden* (Seite 60)).

Zentraler Ausgangspunkt für Benutzer sowie Administratoren für alle weiteren Operationen ist die UCS-Portalseite (siehe *UCS Portalseite* (Seite 57)). Die Portalseite ist standardmäßig auf allen Systemrollen verfügbar und erlaubt einen Überblick über alle in der UCS-Domäne installierten Apps und weiteren Dienste. Alle Aspekte der Portalseite können umfangreich an die eigenen Bedürfnisse angepasst werden (*UCS Portalseite* (Seite 68)).

Für Umgebungen mit mehr als einem Server ist auf der Portalseite ein Verweis auf eine Serverübersichtseite zu sehen.

Diese Unterseite gibt einen Überblick über alle in der Domäne verfügbaren UCS-Systeme. Sie erlaubt die schnelle Navigation hin zu anderen Systemen, um dort z.B. durch UMC-Module Anpassungen an lokalen Einstellungen vorzunehmen.

Univention Management Console (UMC) Module sind das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne, dessen generelle Funktionsweise in *Univention Management Console-Module* (Seite 72) beschrieben wird. Für die Administration der unterschiedlichen Aspekte einer Domäne werden je nach Systemrolle verschiedene Module bereit gestellt. Zusätzlich installierte Software-Komponenten können ihre eigenen UMC-Module mitbringen.

Die anschließenden Abschnitte vertiefen die Benutzung einzelner Aspekte der Domänenverwaltung. *LDAP-Verzeichnis-Browser* (Seite 76) gibt einen Überblick über den LDAP-Verzeichnis-Browser. Die Anwendung von administrativen Einstellungen über Richtlinien wird in *Richtlinien* (Seite 77) besprochen. Wie genau der Funktionsumfangs der Domänenverwaltung erweitert werden kann, ist in *Erweiterung von UMC-Modulen mit erweiterten Attributen* (Seite 79) beschrieben. *Strukturierung der Domäne durch angepasste LDAP-Strukturen* (Seite 83) vertieft, wie Container und Organisationseinheiten (OU) zur Strukturierung des LDAP-Verzeichnisses genutzt werden können. *Delegierte Administration für UMC-Module* (Seite 84) erläutert das Delegieren von Administrationsrechten an weitere Benutzergruppen.

Abschließend wird die Kommandozeilenschnittstelle der Domänenverwaltung dargestellt (*Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)* (Seite 85)) und das Auswerten von Domänendaten über die UCS-Reporting-Funktionalität erläutert (*Auswertung von Daten aus dem LDAP-Verzeichnis mit Univention Directory Reports* (Seite 91)).

Bemerkung: Das UCS Web-Oberfläche ist Teil von Univention Nubus in der *Management UI* Komponente. Weitere Informationen zu Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 2).

4.1 Einführung

4.1.1 Zugriff

Auf jedem UCS-System kann die UCS Web-Oberfläche über die URL `https://servername/` aufgerufen werden. Alternativ ist der Zugriff auch über die IP-Adresse des Servers möglich. Unter besonderen Umständen kann es nötig sein, über eine ungesicherte Verbindung auf die Dienste zuzugreifen (z.B. wenn für das System noch keine SSL-Zertifikate erstellt worden sind). In diesem Fall muss in der URL `http` statt `https` verwendet werden. Passwörter werden in diesem Fall im Klartext über das Netzwerk gesendet!

4.1.2 Browserunterstützung

Die UCS Web-Oberfläche verwendet für die Darstellung zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden unterstützt:

- **`Chrome`** ab Version 85
- **`Firefox`** ab Version 78
- **`Microsoft Edge`** ab Version 88
- **`Safari`** und **`Safari Mobile`** ab Version 13

Auf älteren Browsern können Darstellungsprobleme auftreten oder die Seite funktioniert gar nicht.

Die UCS Web-Oberfläche ist in Deutsch und Englisch verfügbar (und Französisch wenn dieses bei der Installation von DVD als Sprache ausgewählt wurde); die Darstellungssprache kann über den Punkt *Sprache ändern* im Benutzermenü der rechten, oberen Ecke geändert werden.

4.1.3 Zwischen dunklem und hellem Theme für UCS Web-Oberflächen umschalten

Alle UCS Web-Oberflächen haben ein dunkles und ein helles *Theme*, zwischen denen mit der Univention Configuration Registry Variable *ucs/web/theme* (Seite 319) umgeschaltet werden kann. Der Wert von *ucs/web/theme* (Seite 319) entspricht einer CSS Datei unter `/usr/share/univention-web/themes/` mit demselben Namen (ohne Dateierweiterung). Wird *ucs/web/theme* (Seite 319) z.B. auf `light` gesetzt, wird `/usr/share/univention-web/themes/light.css` als *Theme* für alle UCS Web-Oberflächen verwendet.

4.1.4 Erstellen eines eigenen Themes/Anpassen des Designs von UCS Web-Oberflächen

Um ein Thema für UCS Web-Oberflächen anzupassen, bearbeiten Sie nicht die Dateien `/usr/share/univention-web/themes/dark.css` und `/usr/share /univention-web/themes/light.css`, da UCS Upgrades die Änderungen überschreiben können. Kopieren Sie stattdessen eine dieser Dateien z.B. nach `/usr/share/univention-web/themes/mytheme.css` und setzen Sie die Univention Configuration Registry Variable *ucs/web/theme* (Seite 319) auf `mytheme`.

Die Dateien `/usr/share/univention-web/themes/dark.css` und `/usr/share/univention-web/themes/light.css` enthalten die gleiche Liste von CSS Variablen[14]. Andere CSS Dateien verwenden diese CSS Variablen. Diese CSS Variablen sind die unterstützte Konfigurationsschicht für UCS Web-Oberflächen. Die Namen und Anwendungsfälle für diese Variablen ändern sich nicht zwischen UCS Upgrades, aber Univention kann zusätzliche Namen und Anwendungsfälle hinzufügen.

Einige UCS Web-Oberfläches importieren ihre eigene lokale `custom.css` Datei, die Sie verwenden können, um das Design der folgenden Seiten anzupassen:

- Für *Anmelden per Single Sign-On* (Seite 48): `/usr/share/univention-management-console-login/css/custom.css`
- Für *UCS Portalseite* (Seite 68): `/usr/share/univention-portal/css/custom.css`

Die Dateien sind bei der Installation von UCS leer. UCS-Updates ändern diese Dateien nicht.

Wichtig: Beachten Sie jedoch, dass bestimmte CSS-Selektoren[15] bei der Installation eines UCS-Updates kaputt gehen kann.

4.1.5 Feedback zu UCS

Durch die Auswahl des Menüeintrages *Hilfe* ▸ *Feedback* in dem oberen, rechten Menü kann über ein Webformular Feedback zu UCS gegeben werden.

4.1.6 Erfassung von Nutzungsstatistiken

Bei Verwendung der *Core Edition* von UCS (wird generell zur Evaluierung von UCS verwendet) werden anonyme Nutzungsstatistiken zur Verwendung der UCS Web-Oberfläche erzeugt. Weitere Informationen finden sich in KB 6701 - Data collection in Univention Corporate Server[16].

[14] https://developer.mozilla.org/en-US/docs/Web/CSS/CSS_cascading_variables/Using_CSS_custom_properties
[15] https://developer.mozilla.org/en-US/docs/Learn_web_development/Core/Styling_basics/Basic_selectors
[16] https://help.univention.com/t/6701

4.2 Anmelden

UCS stellt eine zentrale Anmeldeseite zur Verfügung. Sie können sich an der UCS Web-Oberfläche mit den Anmeldedaten des jeweiligen Domänenkontos anmelden. Auf dem Portal unter `https://FQDN/univention/portal/` können Sie sich auf folgende Weise anmelden:

- Klicken Sie auf die Kachel *Login* auf der Portalseite.
- Gehen Sie zu *Menu* ▸ *Login*.

Das öffnet die Anmeldeseite wie in Abb. 4.2 gezeigt.

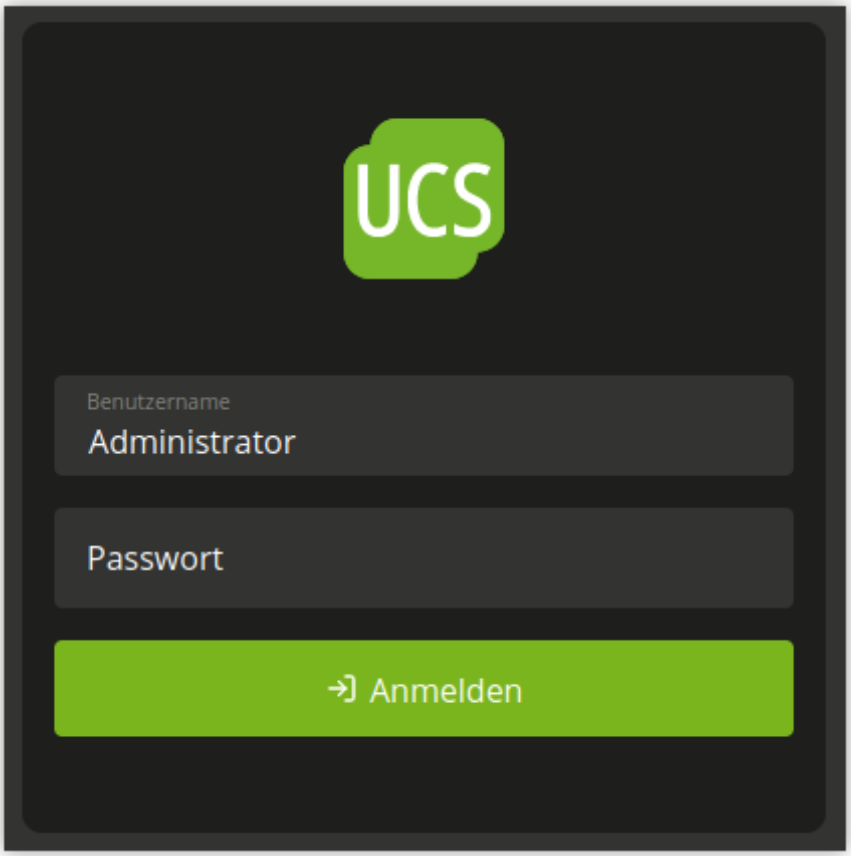


Abb. 4.2: UCS Anmeldeseite

Wenn eine Seite im UCS Managementsystem, z. B. ein UMC-Modul, eine Anmeldung erfordert, leitet Ihr Browser Sie zur zentralen Anmeldeseite weiter.

Wenn Sie sich am lokalen UCS-System anmelden, wird die Sitzung im Browser standardmäßig nach 8 Stunden Inaktivität geschlossen. Sie können den Timeout über die UCR-Variable *umc/http/session/timeout* (Seite 319) ändern. Um eine neue Sitzung zu erhalten, muss sich der Benutzer erneut anmelden.

Um sich aus vom UCS Managementsystem abzumelden, klicken Sie im Benutzermenü auf *Abmelden*.

Durch die Installation einer Anwendung von Drittanbietern, wie z. B. **privacyIDEA**, ist es möglich, die UCS Web-Oberfläche-Authentifizierung um eine Zwei-Faktor-Authentifizierung (2FA) zu erweitern.

4.2.1 Portal Tabs bei Abmeldung aktualisieren

Alle Browser Tabs, in denen der Benutzer im Portal eingeloggt ist, werden automatisch aktualisiert, wenn eine Abmeldung erkannt wird. Diese Funktion ist standardmäßig deaktiviert und kann über die UCR-Variable `portal/reload-tabs-on-logout` umgeschaltet werden.

4.2.2 Wählen Sie das richtige Benutzerkonto

Um sich anzumelden, geben Sie in der Anmeldemaske den *Benutzernamen* und das *Passwort* des entsprechenden Domänenkontos ein.

`Administrator`
: Wenn Sie sich mit dem Konto `Administrator` auf einem Primary Directory Node oder Backup Directory Node anmelden, zeigt das UCS-Managementsystem die UMC-Module für die Verwaltung und Konfiguration des lokalen Systems, sowie die UMC-Module für die Verwaltung der Daten in der Domäne an.

  Sie haben das initiale Passwort für das `Administrator` Konto während der Installation im Setup-Assistenten festgelegt. Das Passwort entspricht dem initialen Passwort des lokalen `root` Kontos. Verwenden Sie das `Administrator` Konto für die Erstanmeldung an einem neu installierten Primary Directory Node.

`root`
: In einigen Fällen kann es notwendig sein, sich mit dem lokalen `root` Konto des Systems anzumelden. Weitere Informationen hierzu finden Sie unter *Administrativer Zugriff mit dem Root-Konto* (Seite 167). Das `root` Konto ermöglicht nur den Zugriff auf UMC-Module für die Verwaltung und Konfiguration des lokalen Systems.

Andere Benutzerkonten
: Wenn Sie sich mit einem anderen Benutzerkonto anmelden, zeigt das UCS Managementsystem die für den Benutzer zugelassenen UMC-Module an. Weitere Informationen zur Zulassung weiterer Module finden Sie unter *Delegierte Administration für UMC-Module* (Seite 84).

4.2.3 Single Sign-On

Standardmäßig ist Single Sign-On auf der Anmeldeseite für das Portal deaktiviert. Die folgenden Abschnitte beschreiben, wie Sie Single Sign-On aktivieren können. Nach erfolgreicher Anmeldung ist die Sitzung für alle UCS-Systeme der Domäne sowie für Applikationen von Drittanbietern gültig, wenn diese webbasiertes Single Sign-On unterstützen.

Bei der einmaligen Anmeldung wird die Browser-Sitzung nach 8 Stunden Inaktivität geschlossen. Um eine frische Sitzung zu erhalten, muss sich der Benutzer erneut anmelden.

Es ist möglich, die Anmeldung auf dem lokalen System zu erzwingen, indem Sie auf den Link *Anmeldung ohne Single Sign On* auf der Anmeldeseite klicken, wie Abb. 4.3 zu sehen.

SAML für Single Sign-On

Bei UCS ist SAML standardmäßig aktiviert. Dieser Abschnitt beschreibt, wie man es für die *Anmeldung* Schaltflächen im Portal aktiviert. Weitere Informationen zu SAML finden Sie unter *SAML Identity Provider* (Seite 46).

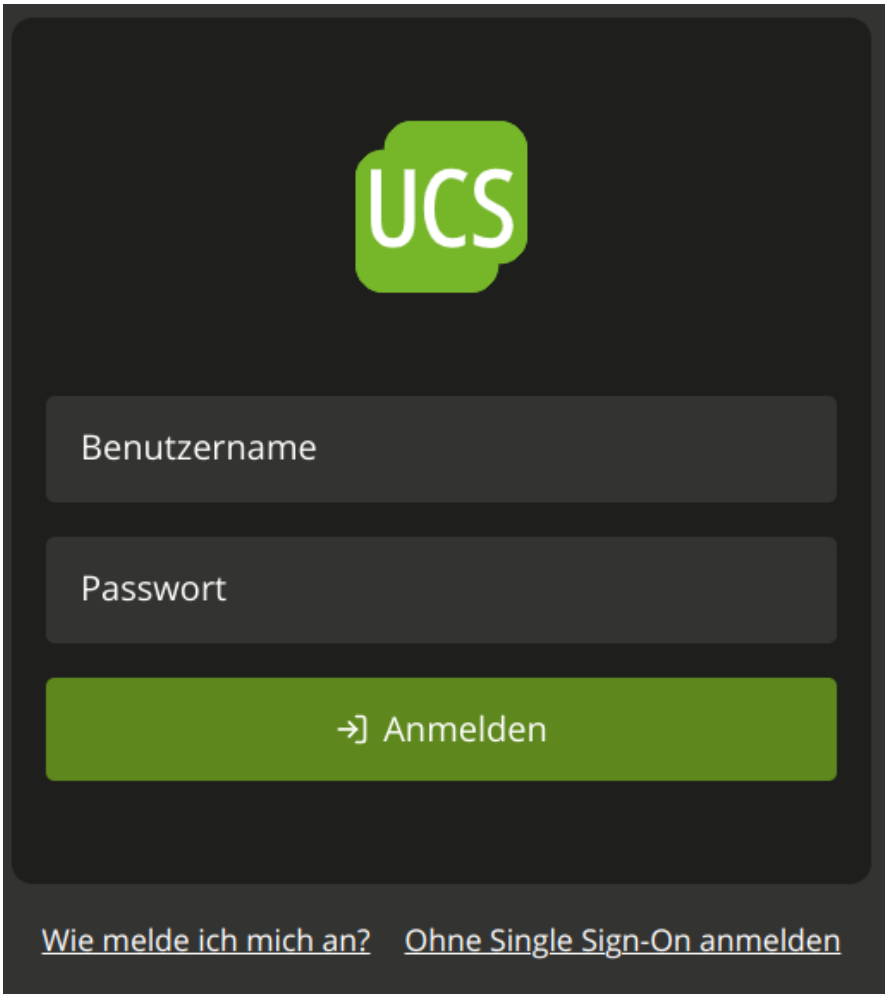


Abb. 4.3: UCS Anmeldeseite für Single Sign-On

Aktivieren

Um Single Sign-On über SAML zu aktivieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass alle Benutzer in Ihrer Domäne, die das Portal und das UCS-Managementsystem mit Single Sign-On nutzen wollen, `ucs-sso.[Domänenname]` erreichen können.
2. Ändern Sie den Univention Configuration Registry Variable *portal/auth-mode* (Seite 315) auf `saml` mit *ucr set* (Seite 163). Der Standardwert war `ucs`.
3. Damit die Änderung wirksam wird, starten Sie den Portal Server mit dem folgenden Befehl neu:

```
$ systemctl restart univention-portal-server.service
```

Anmeldelinks aktualisieren

Der Neustart des Portal Servers aktualisiert automatisch den Link *Anmelden* im Benutzermenü. Sie müssen die Kachel im Portal manuell aktualisieren. Das Standardportal hat eine vorkonfigurierte Kachel zur Anmeldung mit Single Sign-On. Verwenden Sie den Bearbeitungsmodus des Portals, um sie zu aktivieren. Um die Kachel *Anmeldung* durch die Kachel für die einmalige Anmeldung zu ersetzen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie in der *Univention Management Console* das UMC-Modul Portal: *Domäne ▸ Portal*.
2. Um die vorkonfigurierte Kachel zur Anmeldung für SAML zu aktivieren, bearbeiten Sie den Eintrag `login-saml`, scrollen Sie nach unten zum Abschnitt *Erweitert* und aktivieren Sie die Checkbox *Erweitert*.
3. Um die Standard-Kachel zur Anmeldung zu deaktivieren, bearbeiten Sie den Eintrag `login-ucs`, scrollen Sie nach unten zum Abschnitt *Advanced* und deaktivieren Sie die Checkbox *Advanced*.

Um zur Standardanmeldung in UCS ohne Single Sign-On zurückzukehren, müssen Sie müssen Sie die Schritte zum Aktualisieren der Kachel im Portal rückgängig machen und die UCR Variable *portal/auth-mode* (Seite 315) auf `ucs` setzen.

OpenID Connect für Single Sign-On

Neu in Version 5.0-8-erratum-1118: Mit UCS 5.0 erratum 1118[17] haben das Portal und das UCS Management System die Möglichkeit, Single Sign-On mit OpenID Connect durchzuführen. Die Fähigkeit ist standardmäßig deaktiviert.

OpenID Connect (OIDC) ist ein Protokoll, das Single Sign-On ermöglicht. OIDC ist ein einfacheres Protokoll als SAML. Es ist eine Variante für die Verwendung von Single Sign-On im Portal und im UCS-Managementsystem. Dieser Abschnitt beschreibt, wie Sie es mit UCS verwenden.

Anforderungen

Bevor Sie OIDC für Single Sign-On verwenden können, müssen Sie die folgenden Voraussetzungen erfüllen:

1. Sie müssen mindestens UCS 5.0 erratum 1118[18] überall in Ihrer UCS-Domäne installiert haben.

   Informationen zum Upgrade finden Sie unter *Aktualisierung von UCS-Systemen* (Seite 100).

2. Sie müssen die App **Keycloak** in Ihrer UCS-Domäne installiert haben.

   Informationen über die Installation von **Keycloak** finden Sie in Installation[19] in *Univention Keycloak app documentation* [4].

[17] https://errata.software-univention.de/#/?erratum=5.0x1118
[18] https://errata.software-univention.de/#/?erratum=5.0x1118
[19] https://docs.software-univention.de/keycloak-app/latest/installation.html#app-installation

Aktivierung

Zunächst müssen Sie entscheiden, auf welchen UCS-Systemen Sie Single Sign-On mit OpenID Connect aktivieren möchten. Zweitens müssen Sie die folgenden Schritte auf jedem dieser UCS-Systeme anwenden.

1. Deaktivieren Sie SAML für die Anmeldung am Portal über die UCR-Variable *umc/web/sso/enabled* (Seite 319), damit die automatische Neuanmeldung nicht zuerst SAML ausprobiert, sondern direkt OIDC verwendet.

   Ändern Sie die Univention Configuration Registry Variable *umc/web/oidc/enabled* (Seite 319) auf `true` mit *ucr set* (Seite 163).

   ```
   $ ucr set \
      umc/web/sso/enabled=false \
      umc/web/oidc/enabled=true
   ```

2. Führen Sie das Join-Skript für den UMC Webserver aus:

   ```
   $ univention-run-join-scripts \
      --force \
      --run-scripts \
      92univention-management-console-web-server.inst
   ```

3. Ändern Sie den Univention Configuration Registry Variable *portal/auth-mode* (Seite 315) auf `oidc` mit *ucr set* (Seite 163). Der Standardwert war `ucs`.

4. Damit die Änderung wirksam wird, starten Sie den Portal Server mit dem folgenden Befehl neu:

   ```
   $ systemctl restart univention-portal-server.service
   ```

Anmeldelinks erstellen

Durch einen Neustart des Portal Servers wird der *Login*-Link im Benutzermenü automatisch aktualisiert. Optional können Sie mit den Befehlen in Quellcode 4.1 eine Kachel im Portal für die Anmeldung mit OpenID Connect auf dem Primary Directory Node erstellen.

Quellcode 4.1: Portal Kachel für die Anmeldung mit OpenID Connect erstellen

```
$ udm portals/entry create --ignore_exists \
    --position "cn=entry,cn=portals,cn=univention,$(ucr get ldap/base)" \
    --set name=login-oidc \
    --append displayName="\"en_US\" \"Login (Single sign-on)\"" \
    --append displayName="\"de_DE\" \"Anmelden (Single Sign-on)\"" \
    --append description="\"en_US\" \"Log in to the portal\"" \
    --append description="\"de_DE\" \"Am Portal anmelden\"" \
    --append link='"en_US" "/univention/oidc/?location=/univention/portal/"' \
    --set anonymous=TRUE \
    --set activated=TRUE \
    --set linkTarget=samewindow \
    --set icon="$(base64 /usr/share/univention-portal/login.svg)"

$ udm portals/category modify --ignore_exists \
    --dn "cn=domain-service,cn=category,cn=portals,cn=univention,$(ucr get ldap/
↪base)"\
    --append entries="cn=login-oidc,cn=entry,cn=portals,cn=univention,$(ucr get␣
↪ldap/base)"
```

Verifizierung und Logdateien

Um zu überprüfen, ob die Einrichtung funktioniert, öffnen Sie die URL `https://FQDN/univention/oidc/` in einem Webbrowser, z. B. Mozilla Firefox, und melden Sie sich an. Öffnen Sie ein UMC-Modul, z. B. *Users*, und führen Sie eine Suche durch.

Entsprechende Informationen zur Protokollierung finden Sie an den folgenden Stellen:

- Logdatei: `/var/log/univention/management-console.server.log`
- **journald**: **`journalctl -u slapd.service`**

Um die Änderungen für die Anmeldemethode im Portal zu übernehmen, müssen Sie die Kachel *Anmelden* manuell bearbeiten, ähnlich wie bei der Einrichtung mit *SAML für Single Sign-On* (Seite 61). Der Link muss auf `/univention/oidc/` zeigen.

Deaktivieren

Zunächst müssen Sie entscheiden, für welche UCS-Systeme Sie Single Sign-On über OpenID Connect deaktivieren möchten. Zweitens müssen Sie die folgenden Schritte auf jedem dieser UCS-Systeme anwenden.

1. Deaktivieren Sie die Univention Configuration Registry Variable *umc/web/oidc/enabled* (Seite 319) mit *ucr unset* (Seite 164):

```
$ ucr unset umc/web/oidc/enabled
```

2. Entfernen Sie das OIDC RP[20] aus Keycloak mit dem folgenden Befehl:

```
$ univention-keycloak oidc/rp remove \
   "$(ucr get umc/oidc/$(hostname -f)/client-id)"
```

3. Setzen Sie alle Univention Configuration Registry Variablen zurück, die Sie mit den folgenden Suchen finden können:

```
$ ucr search --brief --key ^umc/oidc
$ ucr search --brief --key ^ldap/server/sasl/oauthbearer
```

4. Entfernen Sie das OIDC-Geheimnis aus dem System und starten Sie die betroffenen Dienste neu:

```
$ rm -f \
   /etc/umc-oidc.secret \
   /usr/share/univention-management-console/oidc/http*
$ systemctl restart slapd univention-manangement-console
```

5. Aktualisieren Sie manuell die *Anmelden* Kachel im Portal, so dass der Link auf `/univention/login/` zeigt.
6. Ändern Sie den Univention Configuration Registry Variable *portal/auth-mode* (Seite 315) auf `ucs` mit *ucr set* (Seite 163) und starten Sie den Portal Server neu.

[20] https://docs.software-univention.de/keycloak-app/latest/architecture.html#term-OIDC-RP

Identity Provider mit nicht standardmäßigem FQDN

Standardmäßig ist der FQDN des **Keycloak** Identity Provider `ucs-sso-ng.$domainname`. Jedoch ist es möglich einen anderen FQDN für den Identity Provider zu konfigurieren. Für weitere Informationen, siehe Configuration of the identity provider[21] in *Univention Keycloak app documentation* [4].

Wenn Sie ein solches Setup haben, müssen Sie den Identity Provider für die OpenID-Connect Authentifizierung in UMC auf jedem UCS-System konfigurieren. Ändern Sie die Univention Configuration Registry Variable *umc/oidc/issuer* (Seite 319) in den FQDN Ihres **Keycloak** Identity Provider und führen Sie das Join-Skript des UMC Webservers erneut aus, wie in Quellcode 4.2 gezeigt.

Quellcode 4.2: Nicht standardmäßiger FQDN des **Keycloak** Identity Provider

```
$ IDP="auth.extern.test"
$ ucr set umc/oidc/issuer="https://$IDP/realms/ucs"
$ univention-run-join-scripts --force \
   --run-scripts 92univention-management-console-web-server
```

Univention Portal und UMC mit nicht standardmäßigem FQDN

Standardmäßig ist die UMC über den FQDN `$hostname.$domainname` erreichbar. Falls Sie ein Setup haben, in dem die UMC über einen anderen FQDN erreichbar ist, müssen Sie die Univention Configuration Registry Variable *umc/oidc/rp/server* (Seite 319) auf diesen Wert setzen und das Join-Skript des UMC Webservers nochmals ausführen, siehe Quellcode 4.3.

Quellcode 4.3: Nicht standardmäßigem FQDN für das Portal und die UMC konfigurieren

```
$ ucr set umc/oidc/rp/server="portal.extern.test"
$ univention-run-join-scripts --force \
   --run-scripts 92univention-management-console-web-server
$ systemctl restart slapd
```

Wichtig: Wenn Sie mehrere Portal/UMC-Server hinter einem *Load Balancer* betreiben möchten, müssen Sie diese Befehle auf allen UCS-Systemen ausführen.

Da alle Systeme in diesem Setup denselben OIDC-Client verwenden, stellen Sie sicher, dass die Datei `/etc/umc-oidc.secret` auf jedem System denselben Inhalt hat und mit dem Passwort dieses Clients in **Keycloak** übereinstimmt.

Back-Channel Abmeldung

Wenn Sie die OIDC Back-Channel Abmeldung zusammen mit Multiprocessing der UMC verwenden, benötigt UMC eine Datenbank für die Sitzungsspeicherung, um die Abmeldung korrekt abzuwickeln. Sie haben Multiprocessing in UMC aktiviert, wenn die Univention Configuration Registry Variable `umc/http/processes` einen Wert größer als eins (`> 1`) hat.

Wenn Sie nur einen UMC-Server ohne UMC Multiprocessing haben, können Sie die Konfiguration unverändert belassen.

Damit die UMC die Sitzungen in der Datenbank verwalten kann, müssen Sie die Datenbankverbindung mit dem Skript **univention-mangement-console-settings** konfigurieren, wie in Quellcode 4.5 gezeigt.

[21] https://docs.software-univention.de/keycloak-app/latest/use-cases.html#use-case-custom-fqdn-idp

Wenn das Univention Portal oder die UMC jedoch mehrere UCS-Server zum Lastenausgleich verwenden oder wenn Multiprocessing für UMC konfiguriert sind, ist es notwendig, eine **PostgreSQL** Datenbank zu verwenden, auf die alle UCS-Systeme zugreifen können. In diesen Fällen müssen Sie die folgenden Aspekte berücksichtigen:

1. PostgreSQL Datenbankserver:

   Sie müssen entweder selbst eine **PostgreSQL** Datenbank bereitstellen, auf die alle UMC-Server Zugriff haben.

   Oder Sie installieren und konfigurieren **PostgreSQL** auf einem der UCS-Systeme wie im Beispiel in Quellcode 4.4 gezeigt. Die Werte für `db_user`, `db_name` und `db_password` können Sie frei wählen. `db_host` ist das UCS-System, auf dem **PostgreSQL** läuft.

   Quellcode 4.4: Beispiel für die Installation von **PostgreSQL**

   ```
   $ univention-install univention-postgresql
   $ su postgres -c "createdb db_name"
   $ su postgres -c "/usr/bin/createuser db_user"
   $ su postgres -c "psql db_name -c \"ALTER ROLE db_user WITH ENCRYPTED PASSWORD
   ↪'db_password'\""
   $ ucr set postgres11/pg_hba/config/host="db_name db_user 0.0.0.0/0 md5"
   $ systemctl restart postgresql
   ```

2. Konfiguration der URI für die SQL-Verbindung auf dem Primary Directory Node:

   Quellcode 4.5: Konfiguration der URI für die SQL-Verbindung

   ```
   $ univention-management-console-settings set \
     -u 'postgresql+psycopg2://db_user:db_password@db_host:5432/db_name'
   ```

3. Optionale Einstellungen für den Datenbankverbindungspool:

   - `Pool Size`: Die maximal Anzahl der Datenbank-Verbindungen im Pool. Der Standardwert ist `5`.
   - `Max Overflow`: Die Maximal Anzahl der temporären Verbindungen. Der Standardwert ist `10`.
   - `Pool Timeout`: Die Anzahl der Sekunden, die gewartet werden soll, bis eine Verbindung verfügbar ist. Der Standardwert ist `30`.
   - `Pool Recycle`: Die Anzahl der Sekunden, nach denen Verbindungen im Pool recycelt werden. Der Standardwert ist `-1`.

   Mit diesen Standardwerten kann jeder UMC Prozess bis zu 15 Verbindungen zur Datenbank haben. Die Gesamtzahl der Verbindungen beträgt: `<Anzahl der Server> * <Anzahl der Prozesse> * (<Pool Size> + <Max Overflow>)`. Stellen Sie sicher, dass die Datenbank die Anzahl der Verbindungen verarbeiten kann.

   Quellcode 4.6: Konfiguration der optionalen Parameter für den Datenbankverbindungspool

   ```
   $ univention-management-console-settings set \
       -s 5 \
       -o 10 \
       -t 30 \
       -r 3600
   ```

4. Neustart der UMC auf allen UCS-Servern:

   ```
   $ systemctl restart univention-management-console-server
   ```

Wichtig: Das automatische Aktualisieren der Portal Tabs bei der Abmeldung oder dem Timeout der Sitzung erfordert **PostgreSQL**.

Sie können auch eine lokale **SQLite** Datenbank für einen UMC-Server mit Multiprocessing verwenden, oder Sie können **MariaDB** als zentrale Datenbank für mehrere UMC-Server mit Lastausgleich verwenden. In beiden Fällen wird das Aktualisieren der Portal Tabs nicht unterstützt und funktioniert nicht, da hierfür eine **PostgreSQL** Datenbank erforderlich ist.

4.3 UCS Portalseite

Die Portalseiten dienen der zentralen Darstellung aller verfügbaren Dienste in einer UCS-Domäne. Da sich die Anforderung von kleinen bis hin zu großen Umgebungen in Organisationen, Behörden oder auch im Schulbetrieb stark voneinander unterscheiden, bringt UCS ein sehr flexibles und individuell anpassbares Konzept für Portalseiten mit.

Bemerkung: Das Univention Portal ist Teil von Univention Nubus. Weitere Informationen über Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 2)

Wie in Abb. 4.4 dargestellt, können Portaleinträge (also Verweise auf Applikationen/Apps/Dienste; UDM-Objekttyp `portals/entry`) keinem, einem oder mehreren Portal-Kategorien zugeordnet werden. Eine Portal-Kategorie (UDM-Objekttyp `portals/category`) kann keinem, einem oder mehreren Portalen zugeordnet werden. Ein Portal selbst (UDM-Objekttyp `portals/portal`) stellt alle Portal-Kategorien dar, die mit ihm verknüpft sind.

Darüber hinaus können Sie *Portal Announcements* (Ankündigungen; UDM-Objekttyp `portals/announcement`) erstellen und damit zum Beispiel Wartungsfenster oder Serviceausfälle ankündigen. Ankündigungen können einen Schweregrad wie *Information* oder *Warnung*, ein Start- und Enddatum und eine Einschränkung der Sichtbarkeit auf eine bestimmte Gruppe von Benutzern haben. Eine Ankündigung wird im Portal im oberen Bereich jedes Portals auf allen Portalen angezeigt.

Das Portal *domain*, das mit jeder Installation mitgebracht wird, ist zunächst auf allen UCS-Systemen vorkonfiguriert. Neben allen installierten Applikationen in der Domäne werden hier auch Verweise zu Univention Management Console sowie zur Serverübersicht angezeigt.

Um das anzuzeigende Portal zu ändern, passen Sie die Univention Configuration Registry Variable *portal/default-dn* (Seite 316) an und führen Sie den Befehl **univention-portal update** aus.

Eigene Portale und Portaleinträge können entweder über das UMC-Modul *Portal* oder direkt auf der Portalseite angelegt und verwaltet werden.

Mitglieder der Gruppe `Domain Admins` können nach der Anmeldung am Portal auf dem Primary Directory Node oder Backup Directory Node nach einem Klick auf den entsprechenden Eintrag im Benutzermenü das Portal bearbeiten. Sie können neue Einträge auf dem Portal erstellen, vorhandene Einträge modifizieren, sowie die Reihenfolge oder das Design modifizieren.

Sie können das UMC-Modul *Portal* für erweiterte Einstellungen wie das Erstellen von Portalen und Ankündigungen verwenden oder über die Gruppenmitgliedschaft steuern, welche Benutzer welche Portaleinträge sehen dürfen.

Standardmäßig werden alle Portaleinträge für jeden angezeigt. Im UMC-Modul *Portal* kann für ein Portal in der Kategorie *Anmelden* konfiguriert werden, ob anonyme Besucher sich erst anmelden müssen bevor sie Einträge sehen können. Es ist auch möglich bestimmte Einträge für bestimmte Gruppen zu limitieren. Dies erfordert das LDAP-Attribut `memberOf`. Eine Auswertung von verschachtelten Gruppenmitgliedsschaften (also Gruppen in Gruppen) findet statt.

Weitere Design Anpassungen können Sie in der Datei `/usr/share/univention-portal/css/custom.css` vornehmen. UCS überschreibt diese Datei bei einem Update nicht.

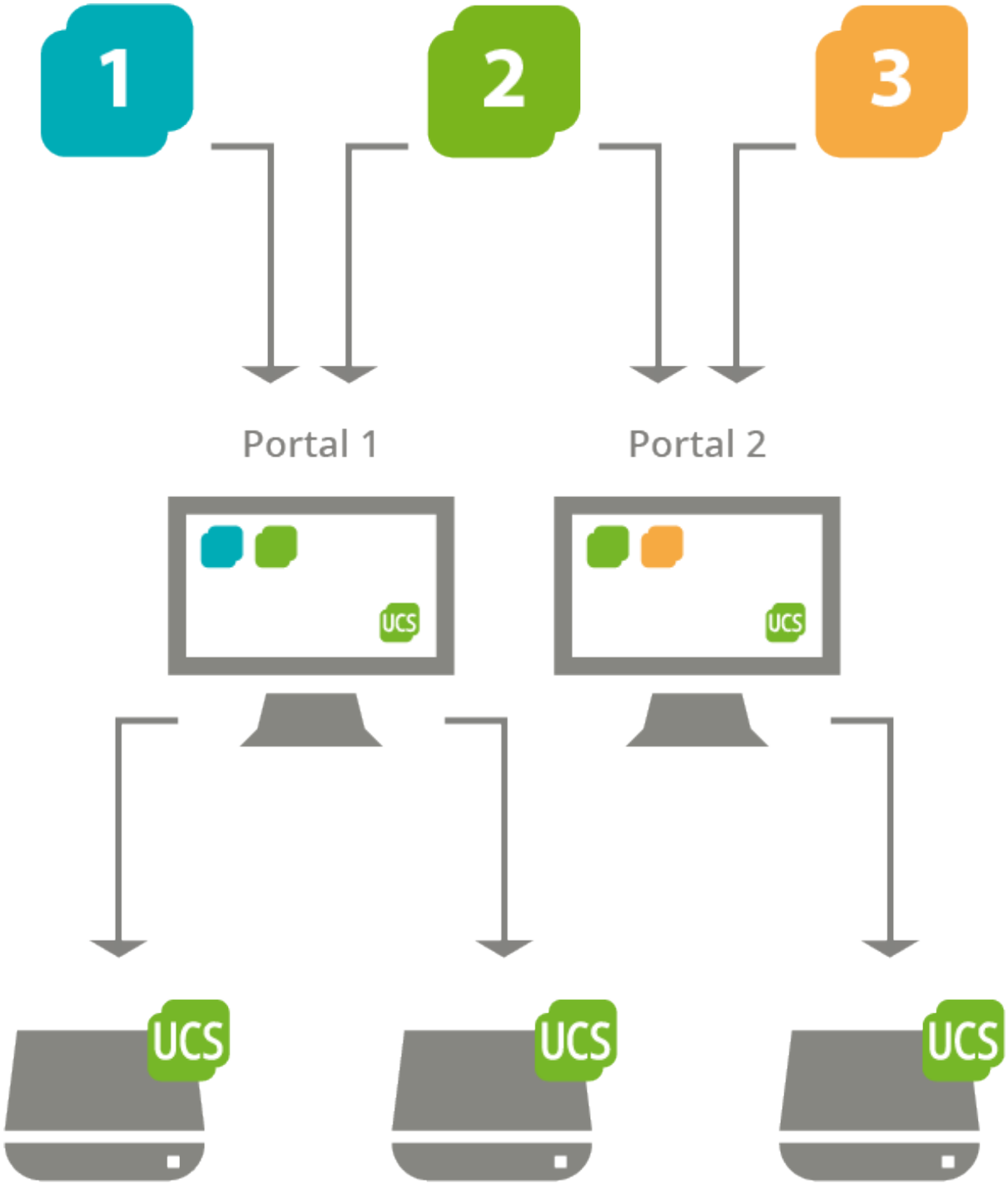


Abb. 4.4: Schema des Portal-Konzepts in UCS: Portale können frei definiert und UCS-Systemen als Startseite zugewiesen werden; ein Verweis kann auf mehreren Portalen angezeigt werden.

4.3.1 Rechte für Portaleinstellungen vergeben

Im Folgenden wird beschrieben, wie das UMC-Modul *Portal* für ausgewählte Gruppen oder Benutzer zugänglich gemacht werden kann. Dies wird anhand eines Beispiels erläutert. Für das Beispiel wird davon ausgegangen, dass eine Gruppe `Portal Admins` erstellt wurde und Mitglieder dieser Gruppe Zugang zu den Portaleinstellungen haben sollen.

Auf einem Primary Directory Node ist zunächst eine ACL-Datei zu erstellen, z.B. `/opt/62my-portal-acl.acl`. Diese Datei hat folgenden Inhalt aufzuweisen, um die nötigen ACL-Änderungen zu ermöglichen:

```
access to dn="cn=portals,cn=univention,@%@ldap/base@%@" attrs=children
  by group/univentionGroup/uniqueMember="cn=Portal Admins,cn=groups,@%@ldap/base@%@
↪" write
  by * +0 break

access to dn.children="cn=portals,cn=univention,@%@ldap/base@%@" attrs=entry,
↪@univentionObject,@univentionNewPortalEntry,
@univentionNewPortal,@univentionNewPortalCategory,children
  by group/univentionGroup/uniqueMember="cn=Portal Admins,cn=groups,@%@ldap/base@%@
↪" write
  by * +0 break
```

Danach ist folgender Befehl auszuführen, um ein LDAP-Objekt für die LDAP-ACLs zu erzeugen:

```
$ udm settings/ldapacl create \
  --position "cn=ldapacl,cn=univention,$(ucr get ldap/base)" \
  --set name=62my-portal-acl \
  --set filename=62my-portal-acl \
  --set data="$(bzip2 -c /opt/62my-portal-acl.acl | base64)" \
  --set package="62my-portal-acl" \
  --set ucsversionstart=4.4-0 \
  --set ucsversionend=5.99-0 \
  --set packageversion=1
```

Wenn die ACL wieder gelöscht werden soll, kann folgender Befehl verwendet werden:

```
udm settings/ldapacl remove \
  --dn "cn=62my-portal-acl,cn=ldapacl,cn=univention,$(ucr get ldap/base)"
```

Über die UMC kann nun eine passende UMC-Richtlinie angelegt werden. Die folgenden *UMC-Operationen* müssen dafür innerhalb der Richtlinie erlaubt werden:

- *udm-new-portal*
- *udm-syntax*
- *udm-validate*
- *udm-license*

Wie man eine Richtlinie anlegt, ist unter *Anlegen einer Richtlinie* (Seite 78) beschrieben. Nun muss die neu erstellte Richtlinie nur noch dem gewünschten Objekt, in diesem Fall der Gruppe `Portal Admins`, zugewiesen werden. Dies kann ebenfalls direkt innerhalb der UMC erfolgen. Für dieses Beispiel navigiert man dafür in das Gruppenmodul und editiert dort die gewünschte Gruppe. In den Gruppeneinstellungen können unter *Richtlinien* für das Gruppenobjekt vorhandene Richtlinien ausgewählt werden. Genauere Informationen über Richtlinienzuweisung sind unter *Zuweisung von Richtlinien* (Seite 78) beschrieben.

4.4 Zustimmung zur Verwendung von Cookies

Sowohl das UCS Portal, als auch die Univention Management Console (UMC), verwenden Cookies und speichern diese auf dem Computer des Benutzers. Abhängig von Ihrem Anwendungsfall und der öffentlichen Präsenz Ihres UCS Portals müssen Sie den Benutzer über die Verwendung von Cookies informieren.

Wenn das Cookie-Banner aktiviert ist, zeigen sowohl UCS-Portal, als auch UMC, ein Banner für die Zustimmung von Cookies an, das der Benutzer akzeptieren muss, um fortzufahren. Sie können den Inhalt mit Univention Configuration Registry Variablen konfigurieren.

4.4.1 Verwendung des Banners für Zustimmung von Cookies

Gehen Sie wie folgt vor, um den Inhalt des Banners für die Zustimmung von Cookies zu aktivieren und anzupassen:

1. Um das Cookie-Banner zu aktivieren, setzen Sie die UCR-Variable *umc/cookie-banner/show* (Seite 71) auf `true`. Das Banner zeigt dann den Standardinhalt an.
2. Um den Titel und den Text anzupassen, setzen Sie die UCR-Variablen *umc/cookie-banner/title* (Seite 71) und *umc/cookie-banner/text* (Seite 72) nach Ihren Wünschen.

   Beachten Sie, dass beide Einstellungen eine sprachspezifische Konfiguration ermöglichen. Weitere Informationen finden Sie im Abschnitt *UCR Referenz für Cookie-Banner* (Seite 71).
3. Sie können optional auch die folgenden Variablen setzen:
   - Der Name des Cookies, wie UCS es auf dem System des Benutzers speichert: *umc/cookie-banner/cookie* (Seite 71).
   - Die Domänen, für die UCS das Cookie-Banner anzeigt: *umc/cookie-banner/domains* (Seite 71).

Das Setzen der entsprechenden UCR-Variablen reicht aus, um das Cookie-Banner zu aktivieren und anzupassen.

Um die Standardtexte wiederherzustellen, deaktivieren Sie die UCR-Variablen *umc/cookie-banner/title* (Seite 71) und *umc/cookie-banner/text* (Seite 72). Um das Cookie-Banner komplett abzuschalten, setzen Sie *umc/cookie-banner/show* (Seite 71) auf `false`.

4.4.2 UCR Referenz für Cookie-Banner

Verwenden Sie die folgenden UCR-Variablen, um das Banner zur Zustimmung von Cookies zu konfigurieren.

umc/cookie-banner/cookie

Die Variable legt den Namen des Cookies fest. In der Voreinstellung ist der Wert leer. UCS verwendet dann den Namen `univentionCookieSettingsAccepted` für das Cookie.

umc/cookie-banner/domains

Optionale Einstellung für die Domänen, für die das Cookie-Banner aktiv ist. Der Wert ist eine durch Kommata getrennte Liste von Domänennamen, für die UCS das Cookie-Banner anzeigt. Bei einer leeren Liste zeigt UCS das Banner für alle Domänennamen an. Die Domäne wird vom Ende der Zeichenkette ausgewertet.

Beispiele:

- Der Wert `example.com` passt zu `portal.example.com` und `sso.example com`. UCS zeigt das Banner für beide Domänennamen an.
- Für den Wert `portal.example.com` zeigt UCS das Cookie-Banner nicht für `sso.example.com`, sondern für `portal.example.com` an.

umc/cookie-banner/show

Die Variable steuert, ob der Browser das Cookie-Banner anzeigt. Der Standardwert ist `false`. Um das Cookie-Banner anzuzeigen, setzen Sie die Variable auf `true`.

umc/cookie-banner/title

Legt den Titel für das Cookie-Banner fest. In der Standardeinstellung ist der Wert leer und UCS bietet einen Standardtitel für Englisch und Deutsch. Verwenden Sie `umc/cookie-banner/title/LANGUAGE` mit einem zweistelligen Sprachcode aus ISO 639-1[22] für *LANGUAGE*, um die Titel für verschiedene Sprachen festzulegen.

umc/cookie-banner/text

Legt den Text für das Cookie-Banner fest. In der Standardeinstellung ist der Wert leer und UCS bietet einen Standardtext für Englisch und Deutsch. Verwenden Sie `umc/cookie-banner/text/LANGUAGE` mit einem zweistelligen Sprachcode aus ISO 639-1[23] für *LANGUAGE*, um Textinhalte für verschiedene Sprachen festzulegen.

4.5 Univention Management Console-Module

Univention Management Console-Module (UMC-Module) sind das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne. Sie werden auf der Portalseite (*UCS Portalseite* (Seite 68)) für angemeldete Administratoren angezeigt. Je nach Systemrolle sind unterschiedliche UMC-Module verfügbar. Zusätzlich installierte Software-Komponenten können ihre eigenen neuen UMC-Module mitbringen.

UMC-Module zur Verwaltung aller im LDAP-Verzeichnis vorgehaltenen Daten (wie z.B. Benutzer, Gruppen oder Rechnerkonten) werden lediglich auf einem Primary Directory Node und Backup Directory Node bereitgestellt. Änderungen, die in diesen Modulen vorgenommen werden, gelten für die gesamte Domäne.

UMC-Module zur Konfiguration und Administration des lokalen Systems werden auf allen Systemrollen bereitgestellt. Über diese Module können z.B. zusätzliche Applikationen installiert, Aktualisierungen eingespielt, die lokale Konfiguration über Univention Configuration Registry angepasst oder Dienste gestartet/gestoppt werden.

4.5.1 Aktivierung der UCS-Lizenz / Lizenz-Übersicht

Die UCS-Lizenz einer Domäne kann dem Primary Directory Node über das UMC-Modul *Willkommen!* verwaltet werden.

Der aktuelle Lizenzstatus kann mit einem Klick auf *Lizenzinfo* angezeigt werden.

Der Schaltfläche *Lizenz importieren* öffnet einen Dialog, über den ein neuer UCS-Lizenzschlüssel aktiviert werden kann (ansonsten greift die standardmäßig installierte Core-Edition-Lizenz). Über die Schaltfläche *Importieren aus Datei…* kann eine Lizenz-Datei ausgewählt und importiert werden. Alternativ kann der Lizenz-Schlüssel auch in das darunter liegende Eingabefeld kopiert und dann über die Schaltfläche *Importieren aus Textfeld* eingespielt werden.

Die Installation der meisten Anwendungen aus dem Univention App Center erfordert einen individuell ausgestellten Lizenzschlüssel mit eindeutiger Schlüsselidentifikation. UCS-Core-Edition-Lizenzen können mit einem Klick auf *Neue Lizenz anfordern* aktualisiert werden. Der aktuelle Lizenzschlüssel wird dabei an Univention geschickt und der aktualisierte Schlüssel nach einigen Minuten an eine angegebene E-Mail-Adresse versendet. Der neue Schlüssel kann dann direkt eingespielt werden. Der Lizenzumfang bleibt durch die Konvertierung unverändert.

Ist die Anzahl der lizenzierten Benutzer- oder Rechner-Objekte überschritten, können keine weiteren Objekte in UMC-Modulen mehr angelegt oder bestehende editiert werden, solange keine erweiterte Lizenz eingespielt wird, oder nicht mehr benötigte Benutzer oder Rechner entfernt werden. Beim Öffnen eines UMC-Moduls wird bei überschrittener Lizenz ein entsprechender Hinweis angezeigt.

[22] https://de.wikipedia.org/wiki/ISO_639#ISO_639-1
[23] https://de.wikipedia.org/wiki/ISO_639#ISO_639-1

Abb. 4.5: Anzeige der UCS-Lizenz

4.5.2 Bedienung der Module zur Verwaltung von LDAP-Verzeichnisdaten

Alle UMC-Module zur Verwaltung von LDAP-Objekten wie z.B. Benutzer-, Gruppen- und Rechnerkonten oder Einstellungen für Drucker, Freigaben, Mail und Richtlinien werden strukturell identisch bedient. Die folgenden Beispiele werden anhand der Benutzerverwaltung dargestellt, gelten aber analog für alle Module. Die Bedienung der DNS- und DHCP-Module weicht etwas ab, weitere Hinweise finden sich in *Konfiguration der DNS-Daten über Univention Management Console Modul* (Seite 222) und *Aufbau der DHCP-Konfiguration durch DHCP-LDAP-Objekte* (Seite 229).

Die inhaltlichen Eigenschaften/Konfigurationsmöglichkeiten der Module ist in folgenden Kapiteln beschrieben:

- Benutzer - *Benutzerverwaltung* (Seite 109)
- Gruppen - *Gruppenverwaltung* (Seite 139)
- Rechner - *Rechnerverwaltung* (Seite 147)
- Netzwerke - *IP- und Netzverwaltung* (Seite 219)
- DNS - *Verwaltung von DNS-Daten mit BIND* (Seite 221)
- DHCP - *IP-Vergabe über DHCP* (Seite 228)
- Freigaben - *Verwaltung von Freigaben* (Seite 247)
- Drucker - *Druckdienste* (Seite 259)
- E-Mail - *Maildienste* (Seite 271)
- Nagios - *Nagios* (Seite 300)

Die Verwendung von Richtlinien (*Richtlinien* (Seite 77)) und das direkte Durchsuchen des LDAP-Verzeichnisbaums (*LDAP-Verzeichnis-Browser* (Seite 76)) werden separat beschrieben.

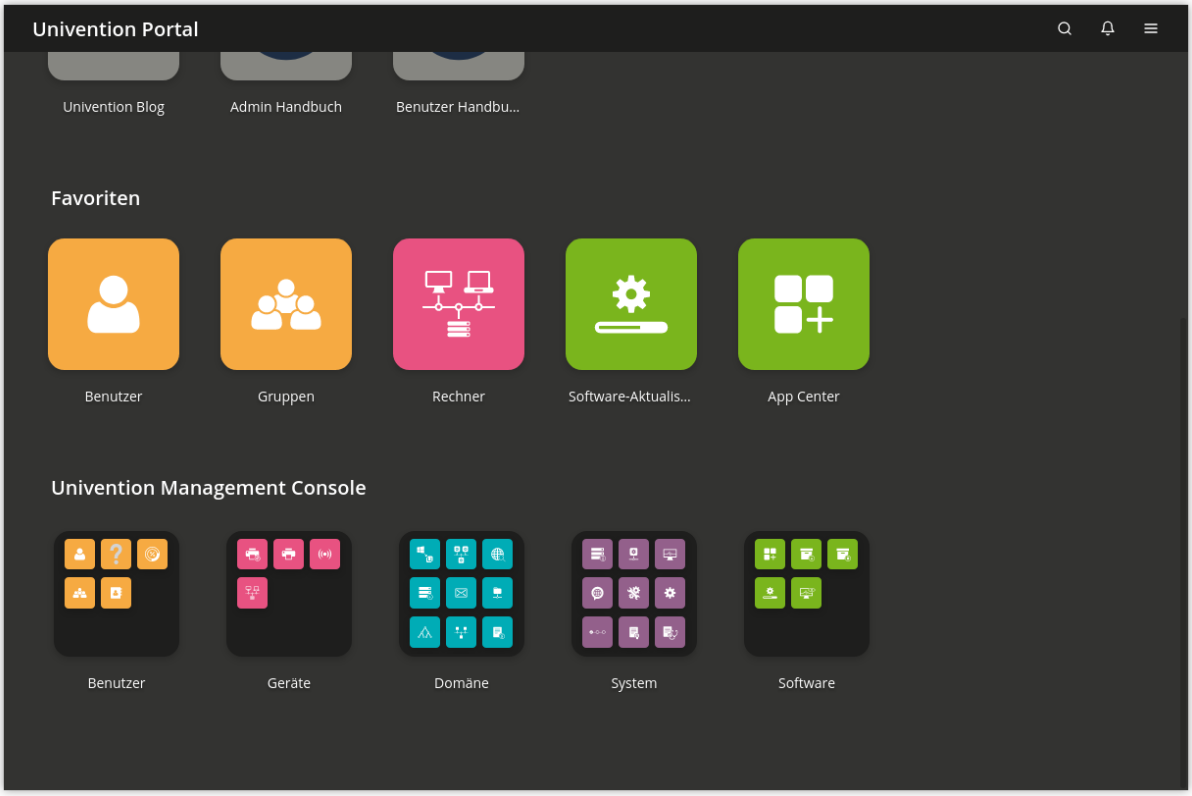


Abb. 4.6: Modulübersicht

Suche nach Objekten

In der Modul-Übersicht werden alle von diesem Modul verwalteten Objekte aufgeführt. Mit *Suche* erfolgt eine Suche über eine Auswahl wichtiger Attribute (z.B. für Benutzerobjekte nach Vor- und Nachname, primärer E-Mail-Adresse, Beschreibung, Mitarbeiternummer und Benutzername). Es kann auch mit Wildcards gesucht werden, z.B. `m*`.

Durch einen Klick auf *Erweiterte Optionen* (das Filter-Icon) werden weitere Suchoptionen angezeigt:

- Mit dem Auswahlfeld *Suche in* kann bestimmt werden, ob bei der Suche nach LDAP-Objekten das komplette LDAP-Verzeichnis oder nur einzelne LDAP-Container/OUs durchsucht werden. Weitere Informationen zur Strukturierung des LDAP-Verzeichnisdienstes finden sich in *Strukturierung der Domäne durch angepasste LDAP-Strukturen* (Seite 83).
- Über das Auswahlfeld *Eigenschaft* kann gezielt nach einem bestimmten Attribut gesucht werden.
- Die meisten Module verwalten mehrere verschiedene Arten von LDAP-Objekten; die Rechnerverwaltung z.B. verwaltet verschiedene Objekte für die einzelnen Systemrollen. Die Suche kann auf eine Art von LDAP-Objekt beschränkt werden.
- Einige nur intern verwendete Benutzer und Gruppen (z.B. für den Domänenbeitritt) werden standardmäßig ausgeblendet. Wird die Option *Versteckte Objekte anzeigen* aktiviert, werden diese Objekte ebenfalls angezeigt.

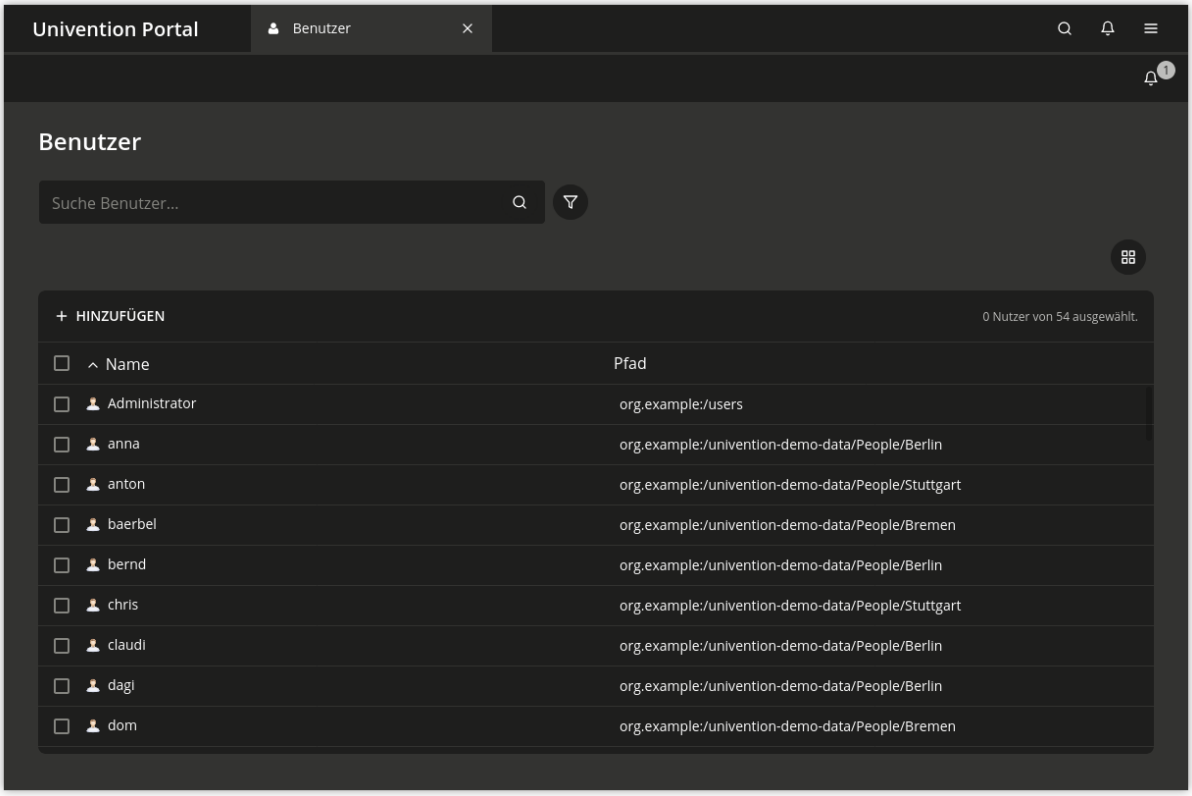


Abb. 4.7: Suche nach Benutzern

Anlegen von Objekten

In der Zeile über der Tabelle mit den Objekten findet sich eine Aktionsleiste, über die mit *Hinzufügen* ein neues Objekt angelegt werden kann.

Für einige UMC-Module (Benutzer, Rechner) existieren vereinfachte Assistenten, in denen nur die wichtigsten Einstellungen abfragt werden. Durch einen Klick auf *Erweitert* werden alle Attribute angezeigt.

Bearbeiten von Objekten

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von *Bearbeiten* kann ein Objekt bearbeitet werden. Die einzelnen Attribute sind in den entsprechenden Abschnitten beschrieben. Mit einem Klick auf *Speichern* ganz oben im Modul werden alle vorgenommenen Anpassungen in das LDAP-Verzeichnis übernommen. Die Schaltfläche *Zurück* bricht die Bearbeitung ab und kehrt zur vorherigen Suchansicht zurück.

Vor jedem Eintrag in der Ergebnisliste ist eine Checkbox, mit dem einzelne Objekte ausgewählt werden können. Der Auswahlstatus wird zusätzlich in der Aktionsleiste der Tabelle dargestellt, z.B. *2 Benutzer von 102 sind ausgewählt*. Ist mehr als ein Objekt selektiert, wird nach einem Klick auf *Bearbeiten* in der Aktionsleiste der Mehrfachbearbeitungsmodus aktiviert. Hierbei werden dieselben Attribute angezeigt wie bei der Bearbeitung eines einzelnen Objekts, Änderungen werden aber nur für die Objekte übernommen, bei denen die *Überschreiben*-Checkbox aktiviert wird. Es können nur Objekte gleichen Typs bearbeitet werden.

Löschen von Objekten

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von *Löschen* wird das Objekt nach Bestätigung einer Rückfrage gelöscht. Einige Objekte verwenden interne Referenzen (z.B. kann zu Rechner-Objekten ein DNS- oder DHCP-Objekt assoziiert werden). Diese können durch Auswahl der Option *Zugehörige Objekte löschen* ebenfalls entfernt werden.

Ähnlich wie beim Bearbeiten mehrerer Objekte auf einmal, können mehrere Objekte auf einmal über die Schaltfläche *Löschen* in der Aktionsleiste gelöscht werden.

Verschieben von Objekten

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von *Verschieben nach…* kann eine LDAP-Position ausgewählt werden, an die das Objekt verschoben werden soll.

Analog zur Auswahl mehrerer Objekte bei der Bearbeitung von Objekten können auch mehrere Objekte auf einmal verschoben werden. Ähnlich wie beim Bearbeiten mehrerer Objekte auf einmal, können mehrere Objekte auf einmal über die Schaltfläche *Mehr* ▸ *Verschieben nach…* in der Aktionsleiste verschoben werden.

4.5.3 Anzeige von Systembenachrichtigungen

UMC-Module können den Benutzer durch Systembenachrichtigungen auf potentielle Fehler wie z.B. nicht ausgeführte Join-Skripte, oder nötige Aktionen wie verfügbare Aktualisierungen hinweisen. Die Benachrichtigungen werden in der oberen rechten Ecke eingeblendet und können erneut mit einem Klick auf das Glockensymbol in der oberen rechten Ecke eingesehen werden.

4.6 LDAP-Verzeichnis-Browser

Über das UMC-Modul *LDAP-Verzeichnis* kann durch das LDAP-Verzeichnis navigiert werden. Dabei können auch Objekte im LDAP-Verzeichnis erzeugt, modifiziert oder gelöscht werden.

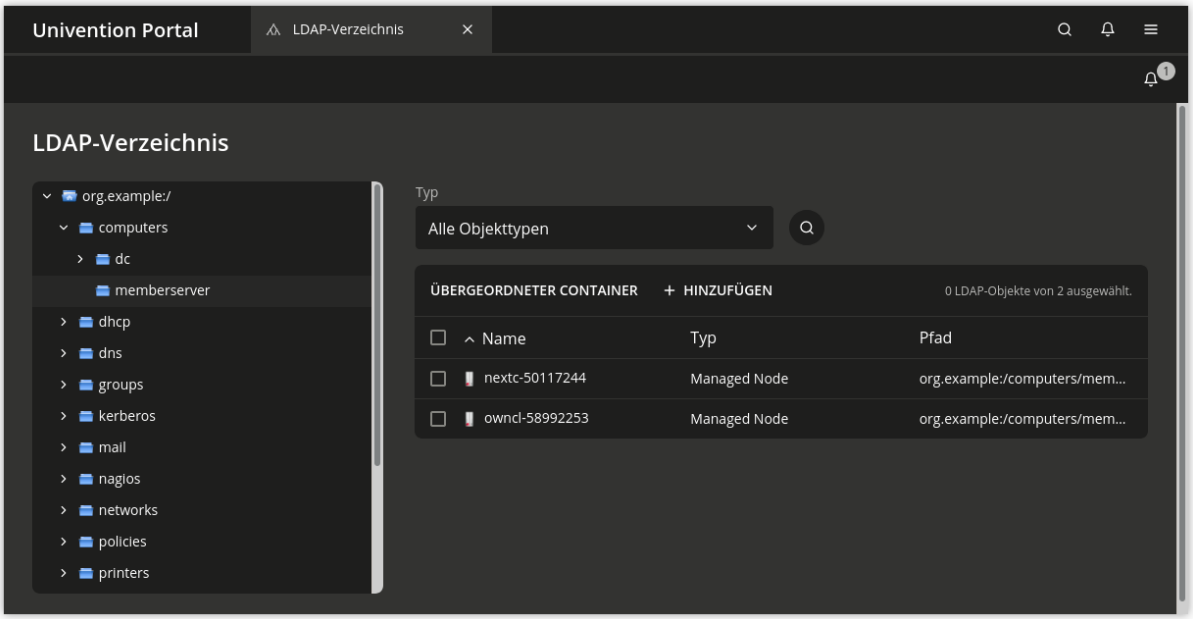


Abb. 4.8: Navigation im LDAP-Verzeichnis

In der linken Bildschirmhälfte ist das LDAP-Verzeichnis in einer Baumstruktur dargestellt, deren Unterelemente durch die Pfeilsymbole ein- und ausgeblendet werden können.

Durch Klick auf ein Element der Baumstruktur wird an diese LDAP-Position gewechselt und in der Übersichtsliste auf der rechten Bildschirmhälfte, die an dieser LDAP-Position befindlichen Objekte angezeigt. Über die Auswahlliste *Typ* kann die Anzeige auf ausgewählte Attribute eingeschränkt werden.

Mit der Schaltfläche *Hinzufügen* können hier auch neue Objekte eingefügt werden. Analog zu den in *Univention Management Console-Module* (Seite 72) beschriebenen Bedienelementen können hier auch bestehende Objekte editiert, gelöscht oder verschoben werden.

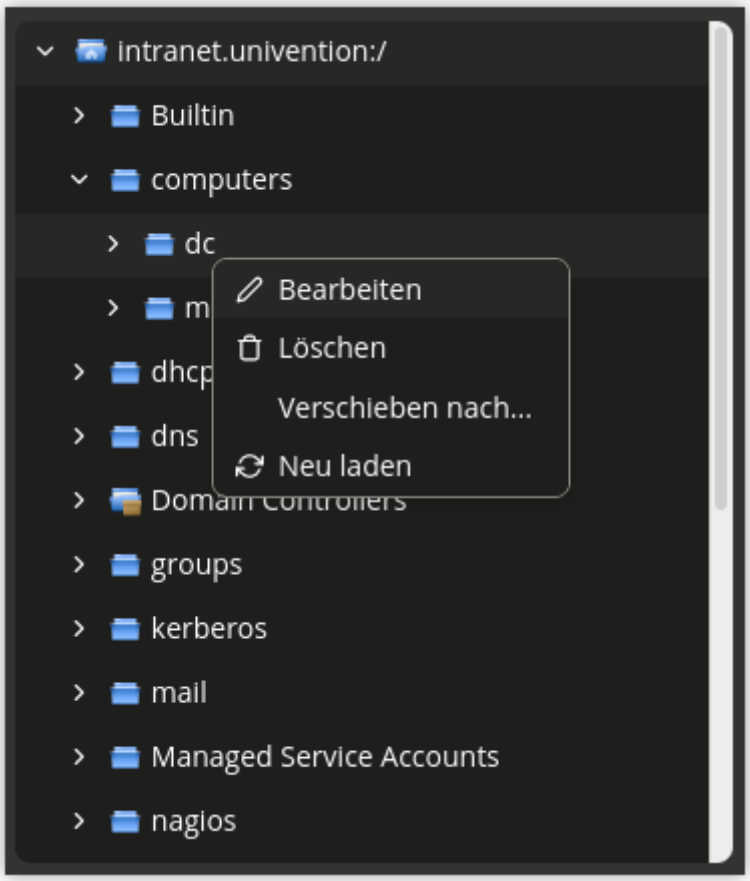


Abb. 4.9: Bearbeiten von LDAP-Container-Einstellungen

Durch Rechtsklick auf ein Element der Baumstruktur können über *Bearbeiten* die Eigenschaften des Containers oder der LDAP-Basis bearbeitet werden.

4.7 Richtlinien

Richtlinien beschreiben administrative Einstellungen, die sinnvoll auf mehr als ein Objekt angewendet werden können. Sie erleichtern die Administration, in dem sie an Container gebunden werden und dann für alle in dem betreffenden Container befindlichen Objekte, sowie die in Unterordnern befindlichen Objekte gelten. Die Einstellungen werden nach dem Prinzip der Vererbung angewendet. Auf ein Objekt wird immer der Wert angewandt, der dem Objekt am nächsten liegt.

Soll z.B. für alle Benutzer eines Standorts das gleiche Passwortablaufintervall definiert werden, kann für diese Benutzer ein eigener Container angelegt werden. Nachdem die Benutzer-Objekte in den Container verschoben wurden, kann eine Passwort-Richtlinie mit dem Container verknüpft werden. Diese Richtlinie gilt für alle enthaltenen Benutzer-Objekte.

Eine Ausnahme bilden Werte, die in einer Richtlinie als *festgelegte Attribute* gesetzt wurden. Diese können von nachgeordneten Richtlinien nicht überschrieben werden.

Mit dem Kommandozeilenprogramm **`univention-policy-result`** kann detailliert angezeigt werden, welche Richtlinie auf ein Verzeichnisdienstobjekt greift.

Jede Richtlinie gilt für einen bestimmten UMC-Domänenobjekttyp, also z.B. für Benutzer oder DHCP-Subnetze.

4.7.1 Anlegen einer Richtlinie

Richtlinien können über das *Richtlinien*-Modul der Univention Management Console verwaltet werden. Die Bedienung erfolgt analog zu den in *Univention Management Console-Module* (Seite 72) beschriebenen Funktionen.

Die Attribute und Eigenschaften der Richtlinien sind in den entsprechenden Kapiteln beschrieben, also die DHCP-Richtlinien beispielsweise im Netzwerk-Kapitel.

Die Namen von Richtlinien dürfen keine Umlaute enthalten.

Unter *Referenzierende Objekte* findet sich eine Aufstellung aller Container oder LDAP-Objekte, mit denen diese Richtlinie aktuell verknüpft ist.

In den erweiterten Einstellungen einer Richtlinie können einige allgemeine Richtlinien-Optionen gesetzt werden, die in der Regel nur für Sonderfälle nötig sind.

LDAP Filter
: Ein LDAP Filter Ausdruck kann hier angegeben werden, der die Anwendung der Richtlinie auf solche Objekte einschränkt, die dem angegebenen Filter genügen.

Benötigte Objektklassen
: Hier können LDAP-Objektklassen angegeben werden, die ein Objekt besitzen muss, damit die Richtlinie auf dieses Objekt greift. Wenn etwa eine Benutzerrichtlinie nur für Windows-Umgebungen relevant ist, könnte hier die Objektklasse `sambaSamAccount` erzwungen werden.

Ausgeschlossene Objektklassen
: Analog zur Konfiguration der benötigten Objektklassen können hier Objektklassen aufgeführt werden, die ausgeschlossen werden sollen.

Festgelegte Attribute
: Hier können Attribute ausgewählt werden, deren Werte von nachgeordneten Richtlinien nicht verändert werden dürfen.

Leere Attribute
: Hier können Attribute ausgewählt werden, die in der Richtlinie leergesetzt, also ohne Wert gespeichert werden sollen. Dadurch können Werte, die ein Objekt von einer übergeordneten Richtlinie ererbt hat, entfernt werden. In nachgeordneten Richtlinien können den Attributen wieder Werte zugewiesen werden.

4.7.2 Zuweisung von Richtlinien

Richtlinien werden Objekten auf zwei unterschiedlichen Arten zugewiesen:

- Eine Richtlinie kann der LDAP-Basis oder einem Container/OU zugewiesen werden. Dazu muss im LDAP-Verzeichnis-Browser (siehe *LDAP-Verzeichnis-Browser* (Seite 76)) in den Eigenschaften des LDAP-Objekts der Reiter *Richtlinien* geöffnet werden.
- In den einzelnen UMC Modulen der LDAP-Verzeichnisobjekte - sofern es für den Typ Richtlinien gibt (z.B. für Benutzer) - wird ein Reiter *Richtlinien* angezeigt. Eine abweichende Richtlinie für einen Benutzer kann an dieser Stelle festgelegt werden.

Der *Richtlinien*-Konfigurationsdialog ist funktional identisch; allerdings werden bei der Zuweisung von Richtlinien an einem LDAP-Container alle Richtlinien-Typen angeboten, während bei der Zuweisung an einem LDAP-Objekt nur die für diesen Objekt-Typ gültigen Richtlinien angeboten werden.

Unter *Richtlinien-Konfiguration* kann dem LDAP-Objekt oder dem Container eine Richtlinie zugewiesen werden. Die aus dieser Richtlinie resultierenden Werte werden direkt angezeigt. Die Einstellung *Ererbt* bedeutet, dass die Einstellungen wieder aus einer übergeordneten Richtlinie - sofern vorhanden - übernommen werden.

Wenn ein Objekt mit einer Richtlinie verbunden ist oder Richtlinien-Einstellungen erbt, die auf das Objekt nicht angewandt werden können, bleiben die Einstellungen ohne Auswirkung für das Objekt. Dadurch ist es z.B. möglich, eine Richtlinie mit der Wurzel des LDAP-Verzeichnisses zu verbinden, die dann für alle Objekte der Domäne, die diese Richtlinie anwenden können, gültig ist. Objekte, die diese Richtlinie nicht anwenden können, werden nicht beeinflusst.

4.7.3 Bearbeiten einer Richtlinie

Richtlinien können im UMC-Modul *Richtlinien* bearbeitet und gelöscht werden. Die Bedienung ist in *Univention Management Console-Module* (Seite 72) beschrieben.

Vorsicht: Beim Bearbeiten einer Richtlinie werden die Einstellungen für alle Objekte, die mit dieser Richtlinie verbunden sind, verändert! Diese Werte aus der geänderten Richtlinie gelten also nicht nur für Objekte, die in der Zukunft hinzugefügt werden, sondern auch für diejenigen, die bereits im System eingetragen und mit der Richtlinie verbunden sind.

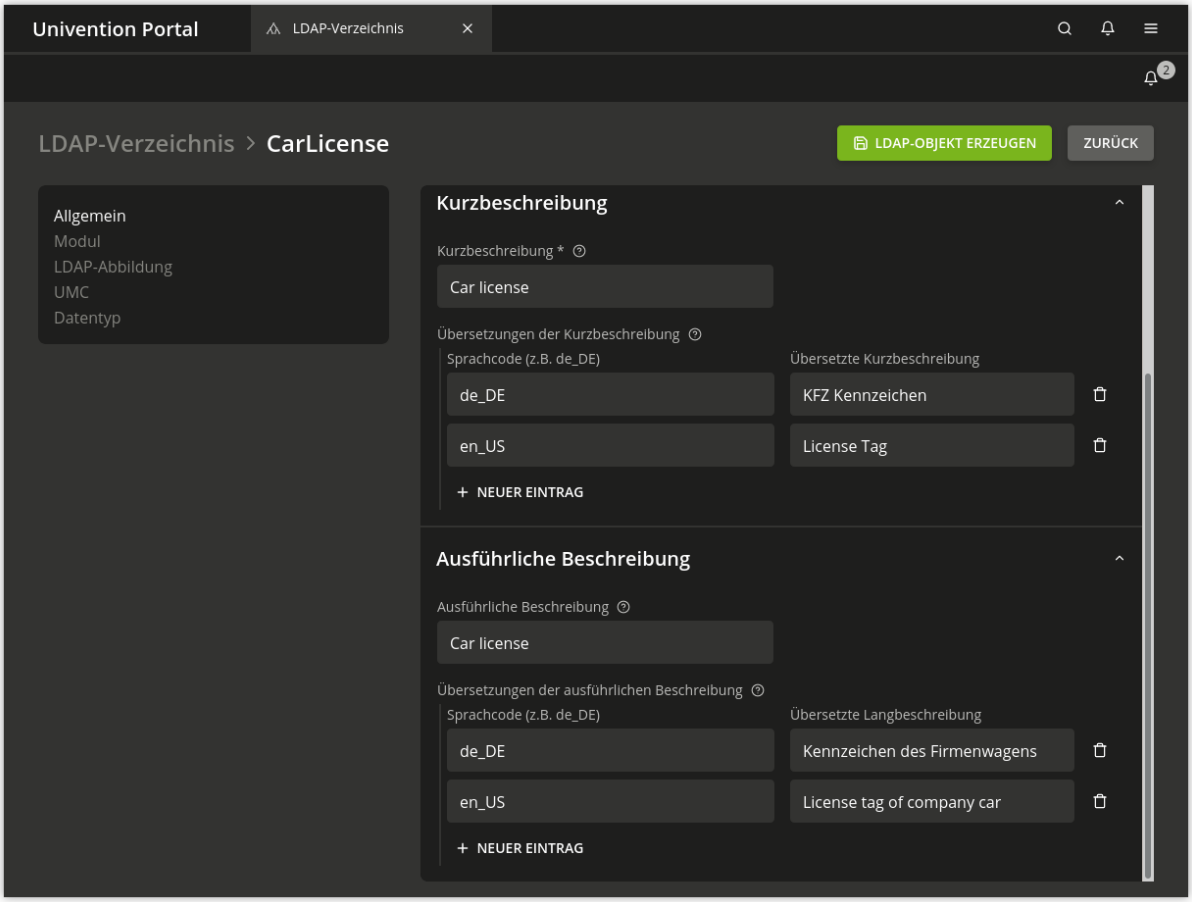
Im Richtlinien-Reiter der einzelnen LDAP-Objekte findet sich außerdem die Schaltfläche *Bearbeiten*, mit der die aktuell für dieses Objekt gültige Richtlinie bearbeitet werden kann.

4.8 Erweiterung von UMC-Modulen mit erweiterten Attributen

Die UMC-Module für die Domänenverwaltung ermöglichen die umfassende Verwaltung der Daten einer Domäne. *Erweiterte Attribute* bieten eine Möglichkeit, neue Attribute in die Domänenverwaltung zu integrieren, die durch den UCS-Standardumfang nicht abgedeckt sind. Erweiterte Attribute werden auch von Drittanbietern für die Integration von Lösungen in UCS eingesetzt.

Erweiterte Attribute werden über das Modul *LDAP-Verzeichnis* verwaltet. Sie befinden sich im Container `univention` und dessen Untercontainer `custom attributes`. Hier können bestehende Attribute bearbeitet werden oder mit *Hinzufügen* ein Objekt vom Typ *Einstellungen: Erweitertes Attribut* angelegt werden.

Erweiterte Attribute können internationalisiert werden. In diesem Fall sollten Namen und Beschreibungen in Englisch verfasst werden, da dies der Standardsprache von UMC-Modulen entspricht.



4.8.1 Erweiterte Attribute - Reiter Allgemein

Tab. 4.1: Reiter *Allgemein*

Attribut	Beschreibung
Eindeutiger Name	Der Name des LDAP-Objektes, als welches das erweiterte Attribut gespeichert wird. Innerhalb eines Containers muss der Name eindeutig sein.
UDM CLI Name	Der angegebene Attributname ist bei der Verwendung der Kommandozeilenschnittstelle Univention Directory Manager zu verwenden. Beim Anlegen des erweiterten Attributs wird hier automatisch *Eindeutiger Name* von der Karteikarte *Allgemein* übernommen und kann nachträglich modifiziert werden.
Kurzbeschreibung	Wird als Überschrift des Eingabefelds in UMC-Modulen oder als Attribut-Beschreibung in der Kommandozeilenschnittstelle verwendet.
Übersetzungen der Kurzbeschreibung	Damit der Titel von erweiterten Attributen auch mit anderen Spracheinstellungen in der jeweiligen Landessprache ausgegeben wird, können übersetzte Kurzbeschreibungen für mehrere Sprachen hinterlegt werden. Dazu kann in diesem Eingabefeld über einen Sprachcode (z.B. `de_DE` oder `fr_FR`) die entsprechend übersetzte Kurzbeschreibung zugeordnet werden.
Ausführliche Beschreibung	Diese erweiterte Beschreibung wird für die Eingabefelder in UMC-Modulen als Tooltip angezeigt.
Übersetzungen der ausführlichen Beschreibung	Zusätzliche Hinweise, die im Tooltip für ein erweitertes Attribut angezeigt werden, können ebenfalls für mehrere Sprachen hinterlegt werden. Dazu kann in diesem Eingabefeld über einen Sprachcode (z.B. `de_DE` oder `fr_FR`) die entsprechend übersetzte Langbeschreibung zugeordnet werden.

4.8.2 Erweiterte Attribute - Reiter Modul

Tab. 4.2: Reiter *Modul*

Attribut	Beschreibung
Zu erweiternde Module	Das Univention Directory Manager-Modul, welches durch das erweiterte Attribut ergänzt werden soll. Ein erweitertes Attribut kann auch für mehrere Module gelten.
Benötigte Optionen/Objektklassen	Einige erweiterte Attribute können nur sinnvoll verwendet werden, wenn auf der Karteikarte *(Optionen)* bestimmte Objektklassen aktiviert sind. In diesem Eingabefeld können optional eine oder mehrere Optionen hinterlegt werden, die am betreffenden Objekt aktiviert sein müssen, damit dieses erweiterte Attribut angezeigt wird oder editierbar ist.
Hook-Klasse	Die Funktionen der hier angegebenen Hook-Klasse werden während des Anlegens, Modifizierens und Löschens von Objekten mit dem erweitertem Attribut aufgerufen. Weiterführende Dokumentation findet sich in der Entwickler-Dokumentation *Univention Developer Reference* [3].

4.8.3 Erweiterte Attribute - Reiter LDAP-Abbildung

Tab. 4.3: Reiter *LDAP-Abbildung*

Attribut	Beschreibung
LDAP-Objektklasse	Die Objektklasse, zu welcher das unter *LDAP-Abbildung* eingetragene Attribut gehört. Für erweiterte Attribute stehen mit der Objektklasse `univentionFreeAttributes` vordefinierte LDAP-Schema-Erweiterungen zur Verfügung. Weitere Hinweise finden sich in *LDAP-Schema-Erweiterungen* (Seite 37). Jedes LDAP-Objekt, das um ein Attribut erweitert werden soll, wird automatisch um die hier angegebene LDAP-Objektklasse erweitert, wenn vom Benutzer ein Wert für das erweiterte Attribut angegeben wurde.
LDAP-Attribut	Der Name des LDAP-Attributs, in dem die Werte am LDAP-Objekt gespeichert werden sollen. Das LDAP-Attribut muss in der angegebenen Objektklasse enthalten sein.
Objektklasse löschen, wenn das Attribut entfernt wird	Wird der Wert für ein erweitertes Attribut in einem UMC-Module gelöscht, wird das Attribut vom LDAP-Objekt entfernt. Werden an diesem LDAP-Objekt keine weiteren Attribute der angegebenen *Objektklasse* verwendet, wird auch die Objektklasse vom LDAP-Objekt entfernt, sofern diese Option aktiviert ist.

4.8.4 Erweiterte Attribute - Reiter UMC

Tab. 4.4: Reiter *UMC*

Attribut	Beschreibung
Dieses erweiterte Attribut nicht in UMC-Modulen anzeigen	Wenn ein Attribut anstatt durch den Administrator nur intern verwaltet werden soll, - z.B. indirekt durch Skripte - kann diese Option aktiviert werden. Das Attribut kann dann nur über das Kommandozeilen-Interface Univention Directory Manager gesetzt werden und wird in UMC-Modulen nicht angezeigt.
Von der UMC-Suche ausschließen	Soll im Suchdialog eines Assistenten nicht nach einem erweiterten Attribut gesucht werden können, kann diese Option aktiviert werden, um das erweiterte Attribut aus der Liste der möglichen Sucheigenschaften zu entfernen. Dies ist nur in Sonderfällen nötig.
Ordnungsnummer	Sollen mehrere erweiterte Attribute auf einer Karteikarte verwaltet werden, kann anhand dieser Positionsnummer die Reihenfolge der Attribute beeinflusst werden. Sie werden in aufsteigender Reihenfolge bestimmt und durch diese Positionsnummer jeweils am Ende der betreffenden Gruppe und Karteikarte angehängt. Fortlaufend vergebene Positionsnummern führen dazu, dass die Attribute jeweils abwechselnd links und rechts zweispaltig angeordnet werden. Ansonsten beginnt die Platzierung in der linken Spalte. Weisen erweiterte Attribute die gleiche Positionsnummer auf, ist deren Reihenfolge zufällig.
Existierendes Eingabefeld überschreiben	In einigen Fällen ist es sinnvoll, vorgegebene Eingabefelder mit erweiterten Attributen zu überschreiben. Wird hier der interne UDM-Name eines Attributs konfiguriert, wird dessen Eingabefeld von diesem erweiterten Attribut überschrieben. Der UDM-Attributname kann mit dem Befehl **`univention-directory-manager`** ermittelt werden (siehe *Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)* (Seite 85)). Es ist zu beachten, dass diese Option bei Pflichtfeldern zu Problemen führen kann.
Beide Spalten umfassen	Alle Eingabefelder werden standardmäßig in zwei Spalten gruppiert. Diese Option kann für überlange Eingabefelder verwendet werden, die sich über die komplette Breite beider Spalten erstrecken sollen.
Name der Karteikarte	Der Name der Karteikarte in UMC-Modulen, auf der das erweiterte Attribut angezeigt werden soll. Hier können auch neue Karteikarten hinzugefügt werden. Wird kein Karteikartenname angegeben, wird *Benutzerdefiniert* verwendet.
Übersetzung des Karteikartennamens	Um den Namen der Karteikarte zu übersetzen, können in diesem Eingabefeld übersetzte Karteikartennamen zum entsprechenden Sprachcode (z.B. `de_DE` oder `fr_FR`) hinterlegt werden.
Existierende Karteikarte überschreiben	Ist diese Option aktiviert, wird die betreffende Karteikarte überschrieben, bevor erweiterte Attribute darauf platziert werden. Mit Hilfe dieser Option können alle vorhandenen Eingabefelder auf einer vorgegebenen Karteikarte ausgeblendet werden. Es ist zu beachten, dass diese Option bei Pflichtfeldern zu Problemen führen kann. Verwendet die zu überschreibende Karteikarte Übersetzungen muss die überschreibende Karteikarte ebenfalls identische Übersetzungen mitbringen.
Karteikarte mit erweiterten Einstellungen	Einstellungsmöglichkeiten, die selten verwendet werden, können auf Karteikarten in den erweiterten Einstellungen platziert werden
Gruppenname	Gruppen ermöglichen die Strukturierung einer Karteikarte. Eine Gruppe wird durch einen grauen Querbalken abgetrennt und kann ein- und ausgeklappt werden. Wird bei einem erweiterten Attribute kein Gruppenname angegeben, wird das erweiterte Attribut oberhalb der ersten Gruppe platziert.
Übersetzung des Gruppennamens	Um den Namen der Gruppe zu übersetzen, können in diesem Eingabefeld übersetzte Gruppennamen zum entsprechenden Sprachcode (z.B. `de_DE` oder `fr_FR`) hinterlegt werden.
Gruppen-Ordnungsnummer	Sollen mehrere Gruppen auf einer Karteikarte verwaltet werden, kann anhand dieser Positionsnummer die Darstellungsreihenfolge beeinflusst werden. Sie werden in aufsteigender Reihenfolge ihrer Positionsnummern dargestellt.

4.8.5 Erweiterte Attribute - Reiter Datentyp

Tab. 4.5: Reiter *Datentyp*

Attribut	Beschreibung
Syntax-Klasse	Bei der Eingabe von Werten nimmt das UMC-Modul eine Syntaxprüfung vor. Neben Standard-Syntaxdefinitionen für Zeichenketten (`string`), Zahlen (`integer`) gibt es drei Möglichkeiten einen binären Zustand auszudrücken: Die Syntax `TrueFalse` wird auf LDAP-Ebene durch die Zeichenketten `true` und `false` abgebildet, die Syntax `TrueFalseUpper` verwendet dagegen die Werte `TRUE` und `FALSE`. Die Syntax `boolean` dagegen speichert keinen Wert oder die Zeichenkette *1*. Standardmäßig wird die Syntax `string` verwendet. Eine Übersicht über die weiteren verfügbaren Syntax-Definitionen und eine Anleitung zur Integration eigener Syntaxen sind in *Univention Developer Reference* [3] zu finden.
Vorgabewert	Ist hier ein Vorgabewert definiert, werden Objekte beim Anlegen mit diesem Wert initialisiert. Der Wert kann während des Anlegens noch manuell bearbeitet werden. Bereits bestehende Objekte werden nicht verändert.
Mehrfachwert	Diese Option legt fest, ob ein einzelner Wert oder mehrere Werte in der Eingabemaske eingetragen werden können. Die Einstellung muss zur Schema-Definition passen, in der für das verwendete LDAP-Attributes festgelegt ist, ob nur eine oder mehrere Instanzen des Attributs an einem LDAP-Objekt verwendet werden dürfen.
Wert wird benötigt	Ist diese Option aktiv, muss ein gültiger Wert für das erweiterte Attribut eingetragen sein, um das betreffende Objekt anzulegen oder zu speichern.
Nachträglich modifizierbar	Diese Option legt fest, ob der im erweiterten Attribut gespeicherte Wert nur während des Anlegens eines Objektes oder auch nachträglich modifiziert werden kann.
Wert wird nur intern verwaltet	Ist diese Option aktiviert, kann das Attribut nicht manuell gesetzt werden, weder beim Anlegen des Objekts, noch nachträglich. Dies ist sinnvoll für automatisch generierte interne Zustände, die über Hook-Funktionen oder intern in einem Modul gepflegt werden.
Kopierbar	Werte dieses erweiterten Attributs werden beim Kopieren eines Objekts automatisch in das Formular eingesetzt.

4.9 Strukturierung der Domäne durch angepasste LDAP-Strukturen

Container und Organisationseinheiten (OU) dienen der Strukturierung der Daten im LDAP-Verzeichnis. Technisch unterscheiden sich beide Typen nicht, sondern eher in der Anwendung:

- Organisationseinheiten repräsentieren in der Regel real existierende Einheiten wie z.B. eine Abteilung einer Firma oder einer Behörde
- Container werden meistens für fiktive Einheiten wie z.B. alle Computer eines Unternehmens verwendet

Container und Organisationseinheiten werden im Modul *LDAP-Verzeichnis* von Univention Management Console verwaltet und werden mit *Hinzufügen* und den Objekt-Typen *Container: Container* und *Container: Organisationseinheit* angelegt.

Container und OUs dürfen prinzipiell an jeder beliebigen Position im LDAP eingefügt werden, OUs können aber nicht unterhalb von Containern angelegt werden.

4.9.1 Reiter Allgemein

Tab. 4.6: Reiter *Allgemein*

Attribut	Beschreibung
Name	Ein beliebiger Name für den Container / die Organisationseinheit.
Beschreibung	Eine beliebige Beschreibung für den Container / die Organisationseinheit.

4.9.2 Reiter Erweiterte Einstellungen

Tab. 4.7: Reiter *Erweiterte Einstellungen*

Attribut	Beschreibung
Zu Standard `[Objekttyp]`-Container hinzufügen	Ist diese Option aktiviert, wird der Container/die Organisationseinheit als Standard-Container für einen bestimmten Objekttyp angesehen. Wird der aktuelle Container etwa als Standard-Benutzercontainer deklariert, wird in den Masken zum Suchen und Anlegen von Benutzern dieser Container ebenfalls angezeigt.

4.9.3 Reiter Richtlinien

Diese Karteikarte wird in *Zuweisung von Richtlinien* (Seite 78) beschrieben.

4.10 Delegierte Administration für UMC-Module

In der Grundeinstellung können nur die Mitglieder der Gruppe `Domain Admins` alle UMC-Module aufrufen. Über Richtlinien kann für Gruppen oder einzelne Benutzer der Zugriff auf UMC-Module konfiguriert werden. Dies kann beispielsweise verwendet werden, um einem Helpdesk-Team die Berechtigung zu erteilen Drucker zu verwalten ohne ihnen Vollzugriff auf die Administration der Domäne zu erteilen.

Die Zuweisung von UMC-Modulen erfolgt über eine *UMC*-Richtlinie (siehe auch *Richtlinien* (Seite 77)), die Benutzer- und Gruppenobjekten zugewiesen werden kann. Die Auswertung erfolgt dabei additiv, d.h. man kann allgemeine Zugriffsrechte durch ACLs auf Gruppenmitgliedschaften erteilen und durch ACLs auf Benutzer ergänzen.

Zusätzlich zu der Zuweisung von UMC-Richtlinien, müssen für UMC-Module, die Daten des LDAP-Verzeichnisses verwalten, ebenfalls LDAP-Zugriffsrechte berücksichtigt werden. Alle im LDAP vorgenommenen Änderungen gelten für die gesamte UCS-Domäne. Daher haben in der Grundeinstellung nur Mitglieder der Gruppe `Domain Admins` sowie einige intern genutzte Konten Vollzugriff auf das UCS-LDAP. Wird ein Modul über eine UMC-Richtlinie freigegeben, muss für den Benutzer/die Gruppe zusätzlich der Zugriff in den LDAP-ACLs freigegeben werden. Weitere Hinweis zu LDAP-ACLs finden sich in *Zugriffskontrolle auf das LDAP-Verzeichnis* (Seite 39).

Tab. 4.8: Richtlinie *UMC*

Attribut	Beschreibung
Liste der erlaubten Operationen	Alle hier definierten UMC-Module werden dem Benutzer oder der Gruppen angezeigt, auf die diese ACL angewendet wird. Die Namen von Domänen-Modulen beginnen mit `UDM`.

Vorsicht: Für den Zugriff auf UMC-Module werden nur Richtlinien ausgewertet, die Gruppen oder aber direkt Benutzer- sowie Rechnerkonten zugewiesen sind. Eine Auswertung von verschachtelten Gruppenmitgliedsschaften (also Gruppen in Gruppen) findet nicht statt.

4.11 Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)

Der Univention Directory Manager ist die Kommandozeilenschnittstelle-Alternative zur webbasierten Schnittstelle der UMC-Module für die Domänenverwaltung. Es dient als mächtiges Werkzeug für die Automatisierung von administrativen Vorgängen in Skripten und zur Integration in andere Programme.

Univention Directory Manager wird als Benutzer `root` auf dem Primary Directory Node mit dem Befehl **`univention-directory-manager`** (Kurzform **`udm`**) aufgerufen.

UMC-Module und Univention Directory Manager verwenden dieselben Domänen-Verwaltungsmodule, d.h. alle Funktionen der Webschnittstelle stehen auch im Kommandozeilen-Interface zur Verfügung.

4.11.1 Aufrufparameter der Kommandozeilenschnittstelle

Eine komplette Liste der verfügbaren Module wird angezeigt, wenn **`udm`** mit dem Parameter `modules` aufgerufen wird:

```
$ univention-directory-manager modules
Available Modules are:
  computers/computer
  computers/domaincontroller_backup
  computers/domaincontroller_master
  computers/domaincontroller_slave
  [...]
```

Für jedes Modul existieren bis zu fünf Operationen:

list
: führt alle existierenden Objekte dieses Typs auf.

create
: legt ein neues Objekt an.

modify
: oder *bearbeitet* existierende Objekte.

remove
: löscht ein Objekt.

move
: zum Verschieben an eine andere Position im LDAP-Verzeichnis.

Die mögliche Optionen eines UDM-Moduls und den darauf anwendbaren Operationen können durch Angabe des Operationsnamens ausgegeben werden, z.B.,

```
$ univention-directory-manager users/user move
[...]
general options:
  --binddn                        bind DN
  --bindpwd                       bind password
  --bindpwdfile                   file containing bind password
[...]
create options:
  --position                      Set position in tree
  --set                           Set variable to value, e.g. foo=bar
[...]
modify options:
  --dn                            Edit object with DN
  --set                           Set variable to value, e.g. foo=bar
[...]
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
remove options:
  --dn                              Remove object with DN
  --superordinate                   Use superordinate module
[...]
list options:
  --filter                          Lookup filter
  --position                        Search underneath of position in tree
[...]
move options:
  --dn                              Move object with DN
  --position                        Move to position in tree
[...]
```

Nähere Informationen, Operationen und Optionen zu jedem Modul gibt der folgende Befehl aus:

```
$ univention-directory-manager [category/modulename]
```

Dabei werden auch die Attribute des Moduls angezeigt. Bei der Operation `create` werden mit `*` die Attribute markiert, die beim Anlegen eines neuen Objektes zwingend angegeben werden müssen.

Einigen Attributen können mehrere Werte zugewiesen werden (z.B. Mailadressen an Benutzerobjekten). Diese Mehrfachwert-Felder sind mit `[]` hinter dem Attributnamen markiert. Einige Attribute können nur gesetzt werden, wenn für das Objekt bestimmte Optionen gesetzt werden. Dies ist bei den einzelnen Attributen durch Angabe des Optionsnamens aufgeführt:

```
users/user variables:
  General:
    username (*)                            Username
[...]
  Contact:
    e-mail (person,[])                      E-Mail Address
```

Hier bezeichnet `username (*)`, dass dieses Attribut beim Anlegen von Benutzerobjekten immer gesetzt werden muss. Wird für das Benutzerkonto die Option *person* gesetzt (dies ist standardmäßig der Fall), können eine oder mehrere E-Mail-Adressen zu den Kontaktinformationen hinzugefügt werden.

Eine Reihe von Standard-Parametern sind für jedes Modul definiert:

`--dn`

Der Parameter wird verwendet, um bei Modifikationen oder beim Entfernen die LDAP-Position des Objektes anzugeben. Dabei muss die komplette DN angegeben werden, z.B,

```
$ univention-directory-manager users/user remove \
  --dn "uid=ldapadmin,cn=users,dc=company,dc=example"
```

`--position`

Um anzugeben, an welcher LDAP-Position ein Objekt angelegt werden soll, wird der Parameter verwendet. Ohne den `--position`-Parameter wird das Objekt unterhalb der LDAP-Basis angelegt! Bei der Operation `move` wird mit diesem Parameter angegeben, an welche Stelle ein Objekt verschoben werden soll, z.B:

```
$ univention-directory-manager computers/ipmanagedclient move \
  --dn "cn=desk01,cn=management,cn=computers,dc=company,dc=com" \
  --position "cn=finance,cn=computers,dc=company,dc=example"
```

`--set`

Der Parameter gibt an, dass dem darauf folgenden Attribut der angegebene Wert zugewiesen wird. Der Parameter muss je Attribut-Wert-Paar verwendet werden, z.B:

```
$ univention-directory-manager users/user create \
  --position "cn=users,dc=compaby,dc=example" \
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
  --set username="jsmith" \
  --set firstname="John" \
  --set lastname="Smith" \
  --set password="12345678"
```

--option

Der Parameter definiert die LDAP-Objektklassen eines Objekts. Wird bei einem Benutzerobjekt beispielsweise nur `pki` als Option übergeben, so kann für diesen Benutzer keine `mailPrimaryAddress` angegeben werden, da dieses Attribut Teil der Option `mail` ist.

--superordinate

`--superordinate` wird zur Angabe von abhängigen, übergeordneten Modulen verwendet. Ein DHCP-Objekt beispielsweise benötigt ein DHCP-Service-Objekt, unter dem es angelegt werden kann. Dieses wird mit der Option `--superordinate` übergeben.

--policy-reference

Mit dem Parameter `--policy-reference` lässt sich Objekten Richtlinien zuweisen (und analog mit `--policy-dereference` entfernen). Wird eine Richtlinie an ein Objekt geknüpft, so werden die Einstellungen aus der Richtlinie für das Objekt angewendet, z.B:

```
$ univention-directory-manager [category | modulename] [Operation] \
  --policy-reference "cn=sales,cn=pwhistory," \
"cn=users,cn=policies,dc=company,dc=example"
```

--ignore-exists

Der Parameter `--ignore_exists` überspringt bereits vorhandene Objekte. Sollte ein Objekt nicht angelegt werden können, da es bereits existiert, wird trotzdem der Fehlercode `0` (kein Fehler) zurückgegeben.

--append

Mit `--append` und `--remove` wird einem Mehrfachwert-Feld ein Wert hinzugefügt/entfernt, z.B:

```
$ univention-directory-manager groups/group modify \
  --dn "cn=staff,cn=groups,dc=company,dc=example" \
  --append users="uid=smith,cn=users,dc=company,dc=example" \
  --remove users="uid=miller,cn=users,dc=company,dc=example"
```

--remove

Siehe *--append* (Seite 87).

4.11.2 Beispielaufrufe für die Kommandozeilenschnittstelle

Die folgenden Beispielaufrufe des Kommandozeilen-Frontend von Univention Directory Manager können als Vorlagen für eigene Skripte verwendet werden.

Benutzer

Anlegen eines Benutzers im Standard-Benutzer-Container:

```
$ univention-directory-manager users/user create \
  --position "cn=users,dc=example,dc=com" \
  --set username="user01" \
  --set firstname="Random" \
  --set lastname="User" \
  --set organisation="Example company LLC" \
  --set mailPrimaryAddress="mail@example.com" \
  --set password="secretpassword"
```

Nachträgliches Hinzufügen der postalischen Adresse zum gerade angelegten Benutzer:

```
$ univention-directory-manager users/user modify \
  --dn "uid=user01,cn=users,dc=example,dc=com" \
  --set street="Exemplary Road 42" \
  --set postcode="28239" \
  --set city="Bremen"
```

Mit diesem Befehl werden alle Benutzer angezeigt, deren Benutzername mit *user* beginnt:

```
$ univention-directory-manager users/user list \
  --filter uid='user*'
```

Die Suche nach Objekten mit `--filter` kann auch auf eine Position im LDAP-Verzeichnis eingeschränkt werden, in diesem Fall auf alle Benutzer im Container `cn=bremen,cn=users,dc=example,dc=com`:

```
$ univention-directory-manager users/user list \
  --filter uid="user*" \
  --position "cn=bremen,cn=users,dc=example,dc=com"
```

Dieser Aufruf entfernt einen Benutzer `user04`:

```
$ univention-directory-manager users/user remove \
  --dn "uid=user04,cn=users,dc=example,dc=com"
```

Eine Firma hat zwei Standorte mit eigens dafür angelegten Containern. Mit dem folgenden Befehl wird ein Benutzer aus dem Container für den Standort „Hamburg“ in den Container für den Standort „Bremen“ verschoben:

```
$ univention-directory-manager users/user move \
  --dn "uid=user03,cn=hamburg,cn=users,dc=example,dc=com" \
  --position "cn=bremen,cn=users,dc=example,dc=com"
```

Gruppen

Anlegen einer Gruppe `Example Users` und Hinzufügen des Benutzers `user01` in diese Gruppe:

```
$ univention-directory-manager groups/group create \
  --position "cn=groups,dc=example,dc=com" \
  --set name="Example Users" \
  --set users="uid=user01,cn=users,dc=example,dc=com"
```

Nachträgliches Hinzufügen des Benutzers `user02` zur gerade angelegten Gruppe:

```
$ univention-directory-manager groups/group modify \
  --dn "cn=Example Users,cn=groups,dc=example,dc=com" \
  --append users="uid=user02,cn=users,dc=example,dc=com"
```

Vorsicht: Ein `--set` des Attributs `users` überschreibt im Gegensatz zu `--append` die Liste der Gruppenmitglieder.

Nachträgliches Entfernen des Benutzers `user01` aus der Gruppe:

```
$ univention-directory-manager groups/group modify \
  --dn "cn=Example Users,cn=groups,dc=example,dc=com" \
  --remove users="uid=user01,cn=users,dc=example,dc=com"
```

Container / Richtlinien

Dieser Aufruf legt unterhalb des Standard-Containers `cn=computers` einen Container `cn=Bremen` für die Rechnerobjekte am Firmenstandort „Bremen“ an. Durch die zusätzliche Option `computerPath` wird dieser Container auch direkt als Standardcontainer für Rechnerobjekte registriert (siehe *Strukturierung der Domäne durch angepasste LDAP-Strukturen* (Seite 83)):

```
$ univention-directory-manager container/cn create \
  --position "cn=computers,dc=example,dc=com" \
  --set name="bremen" \
  --set computerPath=1
```

Dieser Befehl legt eine Speicherplatzbegrenzungsrichtlinie mit dem Namen *Default quota* mit Soft- und Hard-Limit an:

```
$ univention-directory-manager policies/share_userquota create \
  --position "cn=policies,dc=example,dc=com" \
  --set name="Default quota" \
  --set softLimitSpace=5GB \
  --set hardLimitSpace=10GB
```

Diese Richtlinie wird nun an den Benutzer-Container `cn=users` gebunden:

```
$ univention-directory-manager container/cn modify \
  --dn "cn=users,dc=example,dc=com" \
  --policy-reference "cn=Default quota,cn=policies,dc=example,dc=com"
```

Anlegen einer Univention Configuration Registry-Richtlinie, mit der die Vorhaltezeit der Logdateien auf ein Jahr eingestellt wird. Als Trennzeichen zwischen Name und Wert der Variable wird ein Leerzeichen verwendet:

```
$ univention-directory-manager policies/registry create \
  --position "cn=config-registry,cn=policies,dc=example,dc=com" \
  --set name="default UCR settings" \
  --set registry="logrotate/rotate/count 52"
```

Mit diesem Befehl wird an die angelegte Richtlinie ein weiterer Wert angehängt:

```
$ univention-directory-manager policies/registry modify \
  --dn "cn=default UCR settings,cn=config-registry,cn=policies,dc=example,dc=com" \
  --append registry='"logrotate/compress" "no"'
```

Rechner

In folgendem Beispiel wird ein Windows-Client angelegt. Tritt dieser Client später der Samba-Domäne bei (siehe *Windows-Domänenbeitritt* (Seite 32)), wird dieses Rechnerkonto dann automatisch verwendet:

```
$ univention-directory-manager computers/windows create \
  --position "cn=computers,dc=example,dc=com" \
  --set name=WinClient01 \
  --set mac=aa:bb:cc:aa:bb:cc \
  --set ip=192.0.2.10
```

Freigaben

Der folgende Befehl legt eine Freigabe *Documentation* auf dem Server `fileserver.example.com` an. Sofern `/var/shares/documentation/` auf dem Server noch nicht existiert, wird es durch diesen Aufruf auch gleich angelegt:

```
$ univention-directory-manager shares/share create \
  --position "cn=shares,dc=example,dc=com" \
  --set name="Documentation" \
  --set host="fileserver.example.com" \
  --set path="/var/shares/documentation"
```

Drucker

Anlegen einer Druckerfreigabe `LaserPrinter01` auf dem Druckserver `printserver.example.com`. Die Eigenschaften des Druckers sind in der PPD-Datei spezifiziert, deren Name relativ zum Verzeichnis `/usr/share/ppd/` angegeben wird. Der angebundene Drucker ist netzwerkfähig und wird über das IPP-Protokoll angebunden.

```
$ univention-directory-manager shares/printer create \
  --position "cn=printers,dc=example,dc=com" \
  --set name="LaserPrinter01"  \
  --set spoolHost="printserver.example.com" \
  --set uri="ipp:// 192.0.2.100" \
  --set model="foomatic-rip/HP-Color_LaserJet_9500-Postscript.ppd" \
  --set location="Head office" \
  --set producer="producer: cn=HP,cn=cups,cn=univention,dc=example,dc=com"
```

Bemerkung: Zwischen dem Druckprotokoll und dem URL Zielpfad im Parameter `uri` muss ein Leerzeichen stehen. Eine Liste der Druckprotokolle befindet sich in *Konfiguration von Druckerfreigaben* (Seite 260).

Drucker können zur einfacheren Verwaltung in einer Druckergruppe zusammengefasst werden. Weitere Informationen zu Druckergruppen finden sich in *Konfiguration von Druckergruppen* (Seite 263).

```
$ univention-directory-manager shares/printergroup create \
  --set name=LaserPrinters \
  --set spoolHost="printserver.example.com" \
  --append groupMember=LaserPrinter01 \
  --append groupMember=LaserPrinter02
```

DNS/DHCP

Um eine IP-Vergabe über DHCP zu konfigurieren, muss ein DHCP-Rechner-Eintrag für die MAC-Adresse registriert werden. Weitere Informationen zu DHCP finden sich in *IP-Vergabe über DHCP* (Seite 228).

```
$ univention-directory-manager dhcp/host create \
  --superordinate "cn=example.com,cn=dhcp,dc=example,dc=com" \
  --set host="Client222" \
  --set fixedaddress="192.0.2.110" \
  --set hwaddress="ethernet 00:11:22:33:44:55"
```

Soll ein Rechnername über DNS auflösbar sein, kann mit den folgenden Befehlen eine Vorwärts- (host record) und Reverse-Auflösung (PTR record) konfiguriert werden.

```
$ univention-directory-manager dns/host_record create \
  --superordinate "zoneName=example.com,cn=dns,dc=example,dc=com" \
  --set name="Client222" \
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
  --set a="192.0.2.110"

$ univention-directory-manager dns/ptr_record create \
  --superordinate "zoneName=0.168.192.in-addr.arpa,cn=dns,dc=example,dc=com" \
  --set address="110" \
  --set ptr_record="Client222.example.com."
```

Weitere Informationen zu DNS finden sich in *Verwaltung von DNS-Daten mit BIND* (Seite 221).

Erweiterte Attribute

Mit erweiterten Attributen lässt sich der Funktionsumfang von UMC-Modulen flexibel erweitern, siehe *Erweiterung von UMC-Modulen mit erweiterten Attributen* (Seite 79). Im folgenden Beispiel wird ein neues Attribut eingefügt, an dem pro Benutzer das KFZ-Kennzeichen des Dienstwagens gespeichert wird. Die Werte werden in einer extra für diesen Zweck vorgesehenen Objektklasse `univentionFreeAttributes` verwaltet:

```
$ univention-directory-manager settings/extended_attribute create \
  --position "cn=custom attributes,cn=univention,dc=example,dc=com" \
  --set name="CarLicense" \
  --set module="users/user" \
  --set ldapMapping="univentionFreeAttribute1" \
  --set objectClass="univentionFreeAttributes" \
  --set longDescription="License plate number of the company car" \
  --set tabName="Company car" \
  --set multivalue=0 \
  --set syntax="string" \
  --set shortDescription="Car license"
```

4.12 HTTP Schnittstelle (API) der Domänenverwaltung

UCS stellt eine HTTP API für UDM zur Verfügung, mit der UDM Objekte über HTTP-Anfragen überprüft, geändert, erstellt und gelöscht werden können.

Weitere Informationen zur API finden Sie unter *Univention Developer Reference* [3].

4.13 Auswertung von Daten aus dem LDAP-Verzeichnis mit Univention Directory Reports

Univention Directory Reports bietet die Möglichkeit vordefinierte Reports zu beliebigen im Verzeichnisdienst verwalteten Objekten zu erstellen.

Die Struktur der Reports wird dabei durch Vorlagen definiert. Die dafür entwickelte Beschreibungssprache ermöglicht die Verwendung von Platzhaltern, die durch die Werte aus dem LDAP-Verzeichnis ersetzt werden. Es können dabei beliebig viele Reportvorlagen vorgegeben werden. So können beispielsweise für Benutzer wahlweise sehr detaillierte Reports oder nur einfache Adresslisten erstellt werden.

Die Erstellung von Reports ist direkt in die UMC-Module *Benutzer*, *Gruppen* und *Rechner* integriert. Alternativ kann das Kommandozeilenprogramm **`univention-directory-reports`** verwendet werden.

Im Auslieferungszustand werden sechs Reportvorlagen von Univention Directory Reports bereitgestellt, die für Benutzer, Gruppen und Rechner verwendet werden können. Drei Vorlagen erzeugen PDF-Dokumente und drei Vorlagen CSV-Dateien, die als Import-Quelle für andere Programme verwendet werden können. Weitere Vorlagen können erstellt und registriert werden.

4.13.1 Erstellen von Reports in Univention Management Console-Modulen

Um einen Report zu erstellen, muss das UMC-Modul *Benutzer*, *Gruppen* oder *Rechner* geöffnet werden. Anschließend müssen alle vom Report erfassten Objekte ausgewählt werden (durch einen Klick auf die Checkbox links von *Name* können alle Objekte ausgewählt werden). Ein Klick auf *Mehr* ▸ *Report erstellen* ermöglicht die Auswahl zwischen dem *Standard-Report* im PDF-Format und dem *CSV-Report* im CSV-Format.

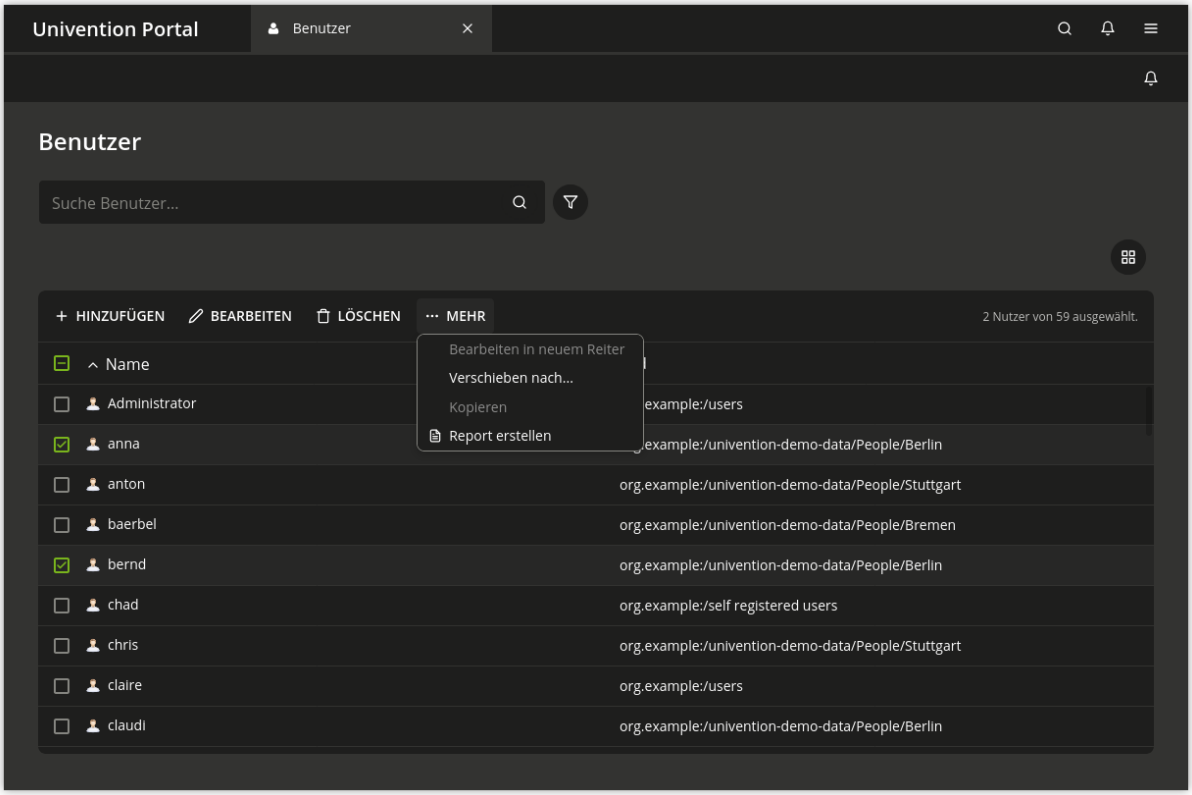


Abb. 4.10: Erstellen eines Reports

Die über die UMC-Module erzeugten Reports werden für 12 Stunden aufbewahrt und danach durch einen Cron-Job entfernt. Die Einstellungen, wann dieser Cron-Job laufen soll und wie lange diese Reports aufbewahrt werden sollen, kann über zwei Univention Configuration Registry-Variablen definiert werden:

directory/reports/cleanup/cron
: Definiert den Zeitpunkt zu dem der Cron-Job ausgeführt werden soll.

directory/reports/cleanup/age
: Bestimmt das maximale Alter eines Report-Dokumentes in Sekunden bevor es gelöscht wird.

4.13.2 Erstellen von Reports auf der Kommandozeile

Reports können auch über die Kommandozeile mit dem Programm **univention-directory-reports** erstellt werden. Informationen zur Verwendung des Programm können über die Option `--help` abgefragt werden.

Mit dem folgenden Befehl können beispielsweise die verfügbaren Reportvorlagen für Benutzer aufgelistet werden:

```
$ univention-directory-reports -m users/user -l
```

4.13.3 Anpassung/Erweiterung von Univention Directory Reports

Schon vorhandene Reports können direkt mit den Voreinstellungen erstellt werden. Einige Voreinstellungen können mittels Univention Configuration Registry angepasst werden. Beispielsweise ist es möglich, das Logo, dass in der Kopfzeile jeder Seite eines PDF-Reports angezeigt wird, zu ersetzen. Dafür kann der Wert der Univention Configuration Registry Variable *directory/reports/logo* (Seite 305) den Namen einer Bilddatei enthalten. Dabei können gängigen Bildformate wie JPEG, PNG oder GIF verwendet werden. Das Bild wird automatisch auf eine feste Breite von 5.0 cm angepasst.

Neben dem Logo kann auch der Inhalt der Reports angepasst werden, indem neue Reportvorlagen definiert werden.

4.14 Let's Encrypt

Let's Encrypt ist eine gemeinnützige Zertifizierungsstelle, die kostenlos X.509 Zertifikate für TLS Verschlüsselung anbietet. Es ist die weltgrößte Zertifizierungsstelle mit dem Ziel, dass alle Webseiten mit HTTPS abgesichert sind.

Die **Let's Encrypt** App im Univention App Center bietet eine weitgehend automatisierte Integration des *acme-tiny Let's Encrypt Clients* in UCS. Unterstützte Dienste in UCS sind der Apache Webserver, der Postfix SMTP Mailserver und der Dovecot IMAP Mailserver.

KAPITEL 5

Softwareverteilung

Die in UCS integrierte Softwareverteilung bietet umfangreiche Möglichkeiten für den Rollout und die Aktualisierung von UCS-Installationen. Sicherheits- und Versionsupdates können über das UMC-Modul *Software-Aktualisierung*, über ein Kommandozeilen-Tool und richtliniengesteuert installiert werden. Dies wird in *Aktualisierung von UCS-Systemen* (Seite 100) beschrieben. Die UCS-Softwareverteilung unterstützt nicht die Aktualisierung von Microsoft Windows-Systemen. Hierfür ist eine zusätzliche Windows-Softwareverteilung nötig.

Für größere Installationen besteht die Möglichkeit, einen lokalen Repository-Server einzurichten, von dem aus alle weiteren Aktualisierungen durchgeführt werden (siehe *Konfiguration des Repository-Servers für Updates und Paketinstallationen* (Seite 102)).

Die UCS-Softwareverteilung basiert auf den unterliegenden Debian-Paketmanagement-Tools, wird aber durch UCS-spezifische Werkzeuge ergänzt. Die verschiedenen Werkzeuge zur Installation von Software werden in *Installation weiterer Software* (Seite 104) vorgestellt. Die Installation von Versions- und Sicherheitsupdates kann über Richtlinien automatisiert werden, siehe *Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie* (Seite 107).

Mit dem Software-Monitor steht ein Werkzeug zur Verfügung, mit dem alle Paketinstallationsstände zentral in einer Datenbank erfasst werden, siehe *Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor* (Seite 107).

Die Erstinstallation von UCS-Systemen ist nicht Bestandteil dieses Kapitels, sie wird stattdessen in *Installation* (Seite 9) beschrieben.

5.1 Unterscheidung der Update-Varianten / Aufbau der UCS-Versionen

Vier Arten von UCS-Updates werden unterschieden:

Major Releases
: *Major Releases* erscheinen ca. alle drei bis vier Jahre. Major Releases können sich von vorhergehenden Major Releases signifikant hinsichtlich ihres Leistungsumfangs, ihrer Funktionsweise und der darin enthaltenen Software unterscheiden.

Minor Releases
: Während der Wartungsdauer eines Major Releases erscheinen *Minor Releases* in einem Rhythmus von ca. 10-12 Monaten. Diese Updates beinhalten die Behebung neu bekannt gewordener Fehler, sowie die Ergänzung des Produkts um zusätzliche Funktionen. Dabei erhalten Minor Releases so weit wie möglich die Kompatibilität zu vorhergehenden Versionen hinsichtlich Funktionsweise, Schnittstellen und Bedienung. Sollte eine Änderung

des Verhaltens sinnvoll oder unvermeidbar sein, so wird bei der Veröffentlichung der neuen Version in den Release Notes darauf hingewiesen.

Patchlevel Releases
Patchlevel Releases fassen ca. alle drei Monate die bis dahin veröffentlichten Errata-Updates zusammen.

Errata Updates
Univention veröffentlicht fortlaufend *Errata-Updates*. Errata-Updates enthalten Korrekturen für Sicherheitslücken und Bugfixes/kleinere Erweiterungen, die zeitnah für Kundensysteme zur Verfügung gestellt werden sollen. Eine Aufstellung aller Errata-Updates findet sich unter https://errata.software-univention.de/.

Jede ausgelieferte UCS-Version besitzt eine eindeutige Versionsbezeichnung. Sie besteht aus einer Zahl (der Majorversion), einem Punkt, einer zweiten Zahl (der Minorversion) einem Bindestrich und einer dritten Zahl (der Patchlevelversion). Mit der Version UCS 4.2-1 wird also das erste Patchlevel-Update für das zweite Minor Update für das Major-Release UCS 4 bezeichnet.

Vor jedem Release-Update wird das *Pre-update-Skript* `preup.sh` aufgerufen. Dieses prüft z.B. ob Probleme bestehen und bricht das Update dann kontrolliert ab. Nach dem Update wird das *Post-Update-Skript* `postup.sh` aufgerufen, das gegebenenfalls weitere Aufräumarbeiten durchführt.

Errata-Updates beziehen sich immer auf bestimmte Minor-Releases, also beispielsweise für UCS 5.0. Errata-Updates können in der Regel für alle Patchlevelversionen eines Minor Releases installiert werden.

Wenn neue Release- oder Errata-Updates verfügbar sind, wird beim Öffnen eines UMC-Moduls ein entsprechender Hinweis ausgegeben. Die Verfügbarkeit neuer Updates wird außerdem per E-Mail angekündigt, entsprechende Newsletter - getrennt nach Release- und Errata-Updates - können auf der Univention-Webseite abonniert werden. Zu jedem Release-Update wird ein Dokument mit Release Notes veröffentlicht, in dem die aktualisierten Pakete, Hinweise zu Fehlerkorrekturen und neuen Funktionen aufgeführt sind.

5.2 Univention App Center

Das Univention App Center erlaubt die einfache Einbindung von Softwarekomponenten in eine UCS-Domäne. Die Applikationen werden sowohl von Drittanbietern wie auch von Univention selbst (z.B. UCS@school) bereitgestellt. Die Software-Pflege und der Support für die Applikationen erfolgt durch den jeweiligen Hersteller.

Das Univention App Center kann über das UMC-Modul *App Center* aufgerufen werden. Es zeigt standardmäßig alle installierten sowie verfügbare Softwarekomponenten an. Mit *Suche Applikationen…* kann die Liste der angezeigten Applikationen auf Suchbegriffe eingeschränkt werden. Außerdem können die Applikationen anhand der *Kategorien* gefiltert werden. Weitere Filterkriterien sind die *App Badges* und die *App Lizenz*. So ist auch eine Kombination der Filter möglich. So kann die Ansicht beispielsweise auf Applikationen aus den Kategorien `Bildung` oder `Office` eingeschränkt werden. Um hieraus dann die *Recommended Apps* anzuzeigen, genügt die Aktivierung des entsprechenden Filters.

Klickt man auf eine der angezeigten Applikationen, werden weitergehende Details zu der Komponente angezeigt, u.a. Beschreibung, Hersteller, Ansprechpartner und Screenshots oder Videos. Im Feld *Benachrichtigung* wird angezeigt, ob der Hersteller der Softwarekomponente bei der Installation/Deinstallation benachrichtigt wird. Ein grobe Einordnung der Lizenzierung kann unter *Lizenz* entnommen werden. Detaillierte Informationen zur Lizenzierung können bei einigen Applikationen direkt über einen *Kaufen* Button bezogen werden. Für alle anderen Applikationen wird die Kontaktaufnahme mit dem Hersteller der Applikation über die unter *Kontakt* angezeigte E-Mail-Adresse empfohlen.

Einige Applikationen sind möglicherweise inkompatibel mit anderen Softwarepaketen aus UCS. So setzen beispielsweise die meisten Groupwarepakete voraus, dass der UCS-Mailstack deinstalliert ist. Jede Applikation prüft, ob inkompatible Versionen installiert sind und gibt einen Hinweis, welche *Konflikte* bestehen und wie sie beseitigt werden können. Die Installation dieser Pakete wird dann zurückgehalten, bis die Konflikte beseitigt sind.

Einige Komponenten integrieren Pakete, die auf dem Primary Directory Node installiert werden müssen (in der Regel LDAP-Schema-Erweiterungen oder Erweiterungen für das UCS-Managementsystem). Diese Pakete werden automatisch auf dem Primary Directory Node installiert. Ist dieser nicht erreichbar, wird die Installation abgebrochen. Außerdem werden die Pakete auf allen erreichbaren Backup Directory Nodes eingerichtet. Sofern mehrere UCS Systeme in der Domäne vorhanden sind, kann ausgewählt werden, auf welchem der Systeme die Applikation installiert werden soll.

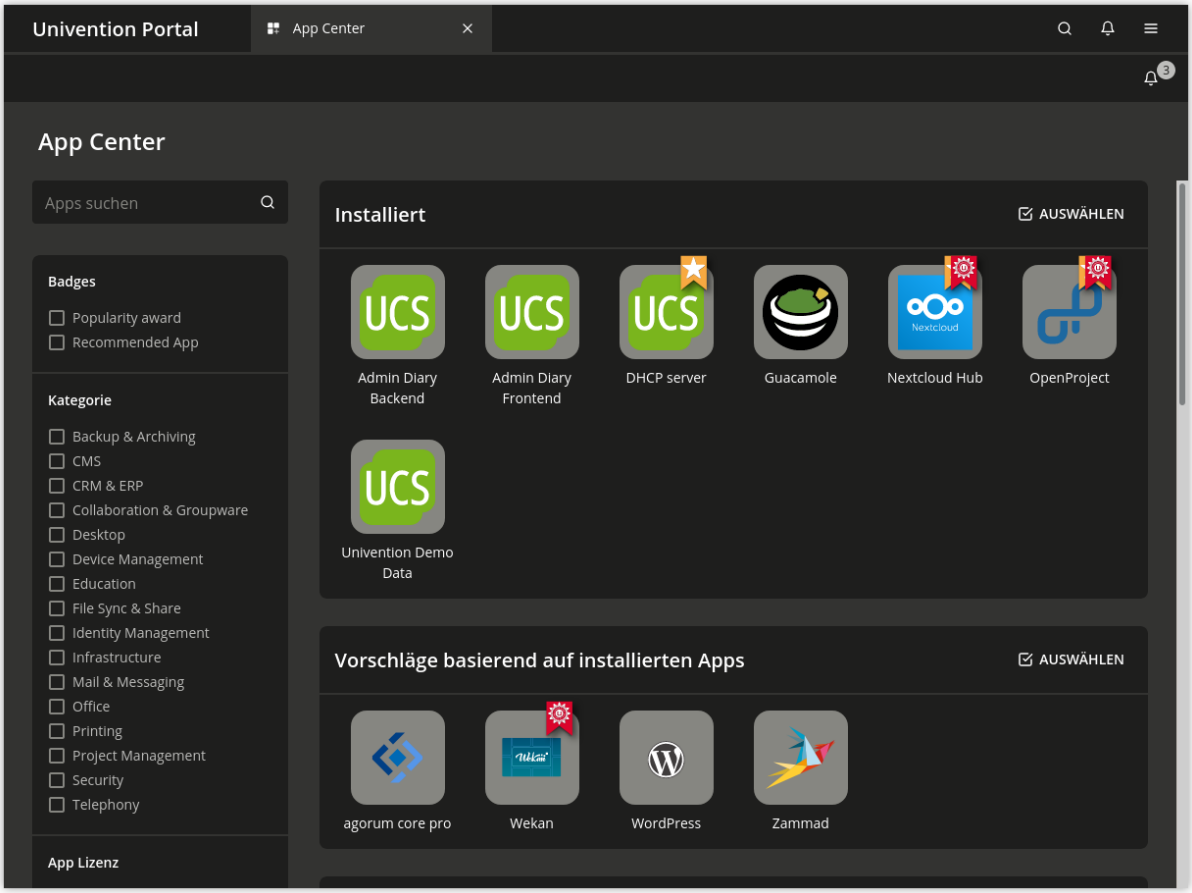


Abb. 5.1: Überblick der verfügbaren Applikationen im App Center

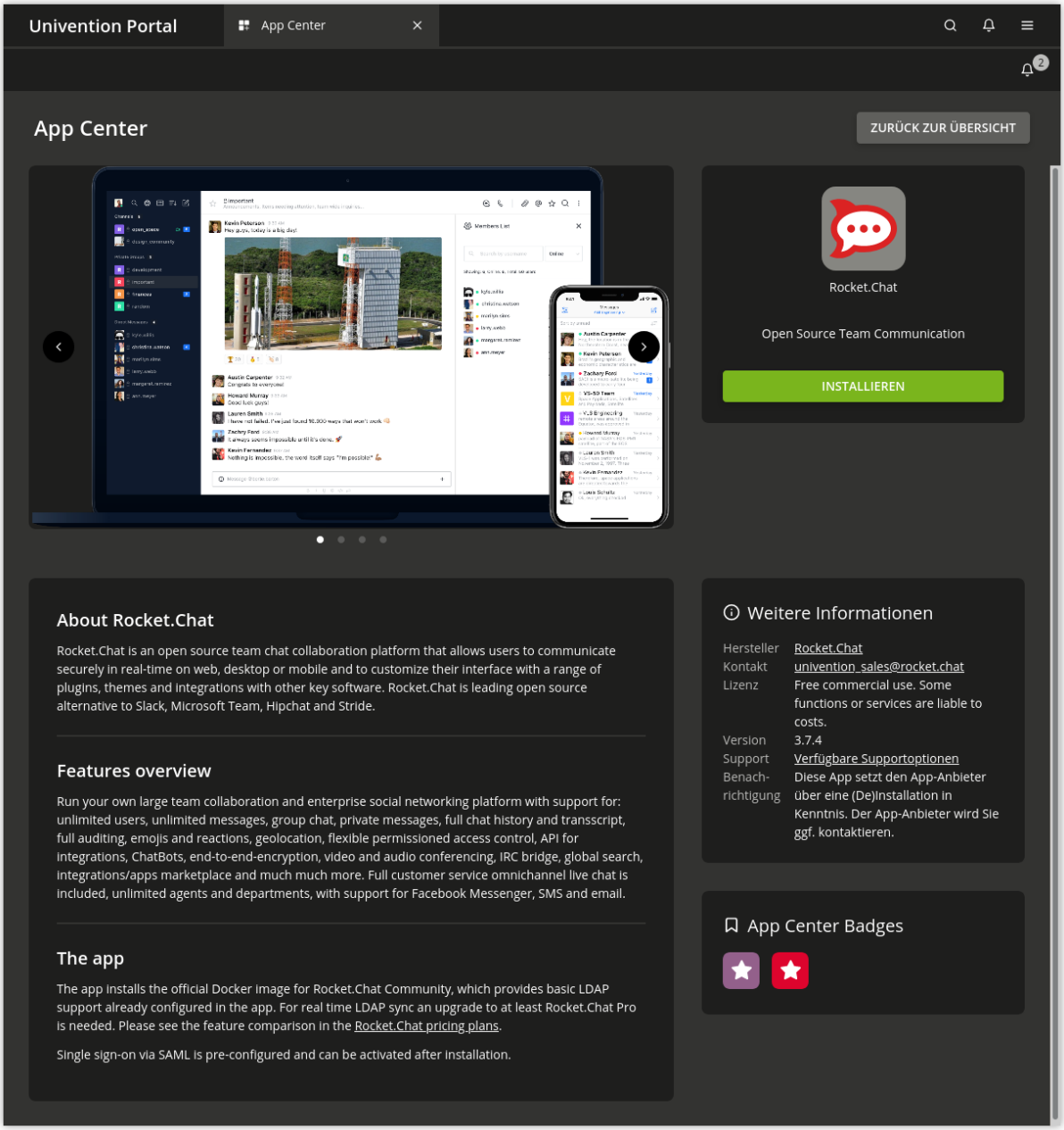


Abb. 5.2: Details einer Applikation im App Center

Einige Applikationen nutzen die Container-Technologie **Docker**. Dadurch wird die Applikation (und ihre unmittelbare Umgebung) vom Rest gekapselt und die Sicherheit sowie die Kompatibilität von Applikationen untereinander erhöht.

Technisch wird die App als Docker Container gestartet und als Managed Node in die UCS Domäne gejoint. Für den Managed Node wird im LDAP ein zugehöriges Rechner-Objekt angelegt.

Der Container ist per Netzwerk nur von dem Rechner aus zu erreichen, auf dem die App installiert ist. Die App kann aber bestimmte Ports öffnen, die dann vom eigentlichen Rechner in den Container weitergeleitet werden. Die Firewall von UCS wird entsprechend automatisch konfiguriert, damit der Zugriff auf die Ports möglich ist.

Wird eine Kommandozeile in der Umgebung der App benötigt, muss zunächst in den Container gewechselt werden. Dazu kann folgender Befehl ausgeführt werden (hier am Beispiel der fiktiven App **demo-docker-app**):

```
$ univention-app shell demo-docker-app
```

Docker Apps lassen sich über das UMC-Modul weiter konfigurieren. Die App kann gestartet und gestoppt, sowie die *Autostart*-Option gesetzt werden:

Automatisch gestartet
: sorgt dafür, dass die App automatisch beim Hochfahren des Servers gestartet wird.

Manuell gestartet
: verhindert den automatischen Start der App, sie kann aber über das UMC-Modul gestartet werden.

Start wird verhindert
: unterbindet grundsätzlich den Start der App; sie kann dann auch nicht über das UMC-Modul gestartet werden.

Darüber hinaus können Apps häufig über weitere Parameter angepasst werden. Das Menü dafür ist über den Button *App-Einstellungen* einer installierten App zu erreichen.

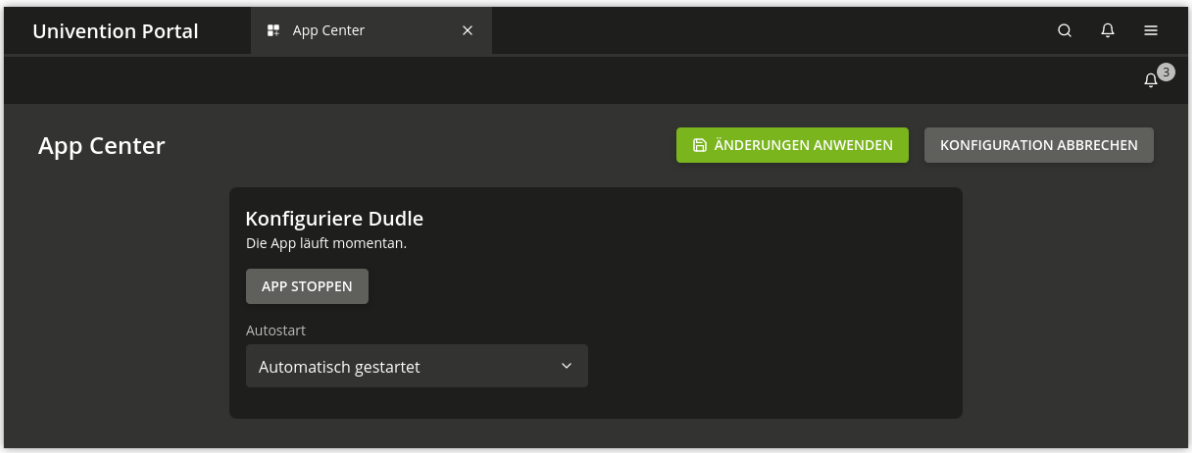


Abb. 5.3: Einstellungen einer Applikation im App Center

Nach der Installation einer Applikation werden beim Klick auf das Icon einer Applikation eine oder mehrere neue Optionen angezeigt:

Deinstallieren
: entfernt eine Applikation.

Öffnen
: verweist auf eine Webseite oder ein UMC-Modul, mit dem die installierte Applikation weitergehend konfiguriert oder verwendet werden kann. Bei Applikationen ohne Webinterface oder UMC-Modul wird die Option nicht angezeigt.

Aktualisierungen für Applikationen erfolgen unabhängig von den Release-Zyklen für Univention Corporate Server. Ist eine neue Version einer Applikation verfügbar, wird der Menüpunkt *Aktualisieren* angezeigt, der die Installation der neuen Version startet. Wenn Aktualisierungen verfügbar sind, wird außerdem im UMC-Modul *Software-Aktualisierung* ein entsprechender Hinweis ausgegeben.

Installationen und das Entfernen von Paketen werden in der Logdatei `/var/log/univention/management-console-module-appcenter.log` protokolliert.

5.3 Aktualisierung von UCS-Systemen

UCS-Systeme können auf zwei Wegen aktualisiert werden; entweder pro einzelnem System (über das UMC-Modul *Software-Aktualisierung* oder auf der Kommandozeile) oder für größere Gruppen von UCS-Systemen automatisiert über eine UMC-Rechner-Richtlinie.

5.3.1 Update-Strategie in Umgebungen mit mehr als einem UCS-System

In Umgebungen mit mehr als einem UCS-System muss die Update-Reihenfolge der UCS-Systeme beachtet werden:

Auf dem Primary Directory Node wird die authoritative Version des LDAP-Verzeichnisdienstes vorgehalten, die an alle übrigen LDAP-Server der UCS-Domäne repliziert wird. Da bei Release-Updates Veränderungen an den LDAP-Schemata auftreten können (siehe *LDAP-Schemata* (Seite 37)) **muss** der Primary Directory Node bei einem Release-Update **immer als erstes System aktualisiert werden**.

Generell ist es empfehlenswert, alle UCS-Systeme möglichst in einem Wartungsfenster zu aktualisieren. Wo dies nicht möglich ist, sollten die nicht-aktualisierten UCS-Systeme gegenüber dem Primary Directory Node nur eine Release-Version älter sein.

5.3.2 Aktualisierung eines einzelnen Systems im Univention Management Console Modul Software-Aktualisierung

Mit dem UMC-Modul *Software-Aktualisierung* können Versions- und Errata-Updates installiert werden.

Abb. 5.4 zeigt die Übersichtsseite des Moduls. Im oberen Teil des Dialogs wird unter *Release-Aktualisierungen* der aktuelle Installationsstand angezeigt.

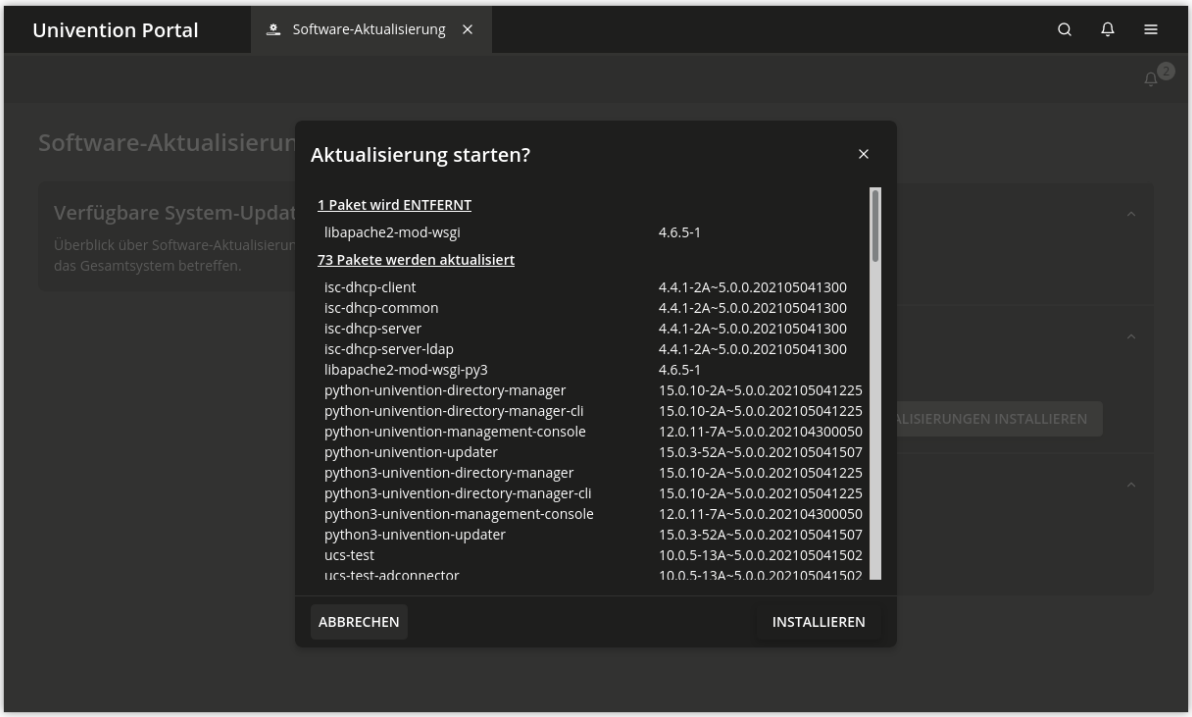


Abb. 5.4: Aktualisierung eines UCS-Systems über das UMC-Modul *Software-Aktualisierung*

Sollte eine neuere UCS-Version vorhanden sein, wird eine Auswahlliste präsentiert. Durch einen Klick auf *Release-Aktualisierungen installieren* werden nach Bestätigung alle Updates bis zur jeweiligen Version eingespielt. Zuvor wird ein Hinweis auf mögliche Einschränkungen der Serverdienste während des Updates angezeigt. Eventuelle Zwischenversionen werden automatisch mitinstalliert.

Durch einen Klick auf *Errata-Aktualisierungen installieren* werden alle für das aktuelle Release und die eingebundenen Komponenten verfügbaren Errata-Updates eingerichtet.

Mit *Paket-Aktualisierungen prüfen* wird eine Aktualisierung der momentan eingetragenen Paketquellen aktiviert. Dies kann etwa verwendet werden, wenn für eine Komponente eine aktualisierte Version bereitgestellt wurde.

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.3.3 Aktualisierung eines einzelnen Systems auf der Kommandozeile

Die folgenden Schritte müssen mit `root`-Rechten durchgeführt werden.

Ein einzelnes UCS-System kann auf der Kommandozeile mit dem Befehl **`univention-upgrade`** aktualisiert werden. Es wird geprüft, ob neue Release- oder Applikationsupdates vorliegen, die dann nach Bestätigung einer Nachfrage installiert werden. Außerdem werden Paket-Aktualisierungen durchgeführt, z.B. im Rahmen eines Errata-Updates.

Von einer Remote-Aktualisierung über SSH wird abgeraten, da dies zum Abbruch des Update-Vorgangs führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können beispielsweise die Tools **`screen`** oder **`at`** eingesetzt werden, die auf allen Systemrollen installiert sind.

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.3.4 Aktualisierung von Systemen über eine Rechner-Richtlinie

Mit einer *Automatische Updates*-Richtlinien im UMC-Modul *Rechner* lässt sich ein Update für mehrere Rechner konfigurieren (siehe auch *Richtlinien* (Seite 77)).

Nur wenn das Auswahlfeld *Aktiviere Release-Updates* aktiviert ist, wird eine Release-Aktualisierung durchgeführt.

Das Eingabefeld *Bis zu dieser UCS-Version aktualisieren* enthält die Versionsnummer, bis zu der das System aktualisiert werden soll, z.B. `5.0-0`. Wird keine Angabe gemacht, aktualisiert sich das System bis zur höchsten verfügbaren Versionsnummer.

Der Zeitpunkt, zu dem die Aktualisierung durchgeführt wird, wird über eine *Paketpflege*-Richtlinie konfiguriert (siehe *Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie* (Seite 107)).

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.3.5 Nachbereitung von Release-Updates

Nach erfolgreicher Durchführung eines Release-Updates sollte geprüft werden, ob neue oder aktualisierte Join-Skripte ausgeführt werden müssen.

Zur Überprüfung und zum Starten der Join-Skripte kann entweder das UMC-Modul *Domänenbeitritt* verwendet werden oder das Kommandozeilenprogramm **`univention-run-join-scripts`** (siehe *Domänenbeitritt von UCS-Systemen* (Seite 30)).

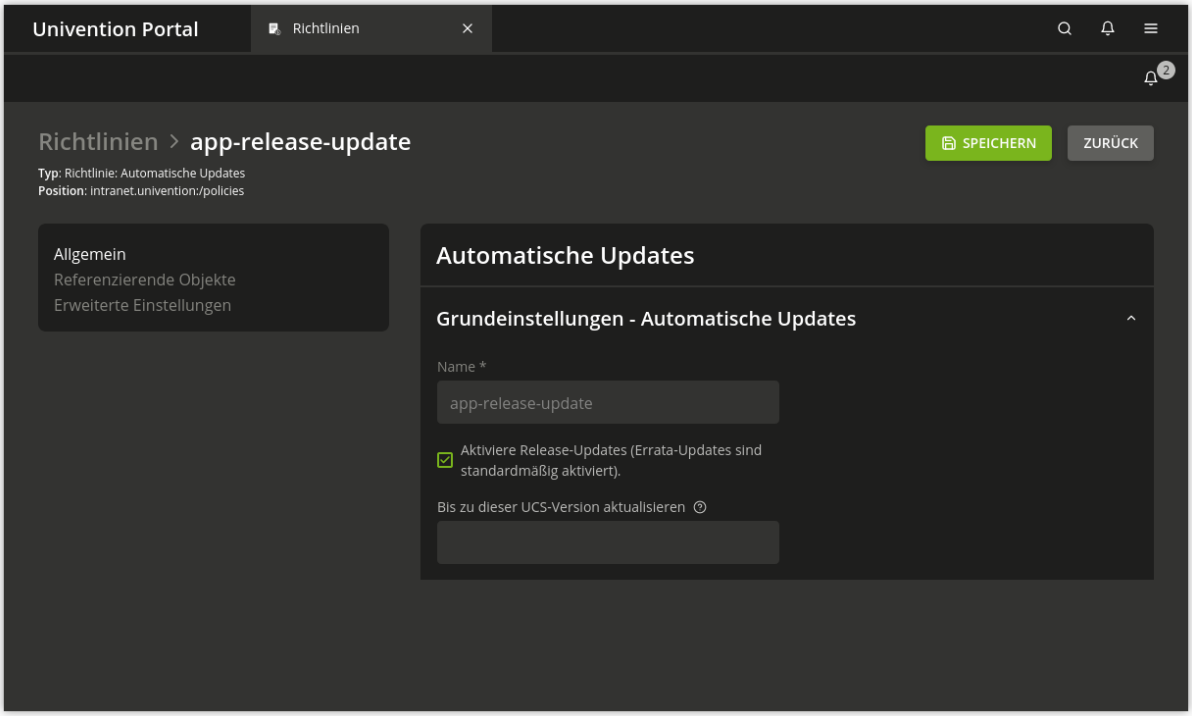


Abb. 5.5: Aktualisierung eines UCS-Systems über eine Update-Richtlinie

5.3.6 Fehlersuche bei Updateproblemen

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben, die zur weiteren Fehleranalyse herangezogen werden kann.

Der Stand der Univention Configuration Registry-Variablen vor der Release-Aktualisierung wird in dem Verzeichnis `/var/univention-backup/update-to-ZIELRELEASEVERSION/` gesichert. Damit kann geprüft werden, ob und welche Variablen im Rahmen des Updates verändert wurden.

5.4 Konfiguration des Repository-Servers für Updates und Paketinstallationen

Paketinstallationen und Updates können entweder vom Univention-Update-Server oder von einem lokal gepflegten Repository durchgeführt werden. Ein lokales Repository ist sinnvoll, wenn viele UCS-Systeme zu aktualisieren sind, da Updates in diesem Fall nur einmalig heruntergeladen werden müssen. Da Repositorys auch offline aktualisiert werden können, ermöglicht ein lokales Repository auch die Aktualisierung von UCS-Umgebungen ohne Internetanbindung.

Ein lokales Repository kann viel Plattenplatz in Anspruch nehmen.

Anhand der registrierten Einstellungen werden APT-Paketquellen für Release- und Errata-Updates sowie Addon-Komponenten im Verzeichnis `/etc/apt/sources.list.d/` automatisch generiert. Sollten auf einem System weitere Repositorys benötigt werden, können diese in die Datei `/etc/apt/sources.list` eingetragen werden.

Bei einer Neuinstallation wird in der Grundeinstellung das Univention-Repository `updates.software-univention.de` verwendet.

Das Univention Repository enthält alle von Univention und Debian bereitgestellten Pakete. Dabei wird zwischen maintained und unmaintained Paketen unterschieden.

- Alle Pakete im Standard-Paketumfang befinden sich im Status *maintained*. Sicherheitsupdates werden zeitnah nur für *maintained* Pakete bereitgestellt. Die Liste der *maintained* Pakete ist auf einem UCS System unter `/usr/share/univention-errata-level/maintained-packages.txt` einsehbar.
- *unmaintained* Pakete sind nicht durch Sicherheitsupdates oder anderweitige Maintenance abgedeckt. Um zu prüfen ob *unmaintained* Pakete installiert sind, kann das Kommando **univention-list-installed-unmaintained-packages** ausgeführt werden.

Für zusätzliche eingebundene Repositories ist die Installation von *unmaintained* Paketen standardmäßig nicht möglich. Um die Installation zu ermöglichen, muss die Univention Configuration Registry Variable *repository/online/component/.*/unmaintained* (Seite 316) auf `yes` gesetzt werden.

5.4.1 Konfiguration über Univention Management Console Modul

Im UMC-Modul *Repository-Einstellungen* kann der *Repository-Server* festgelegt werden.

5.4.2 Konfiguration über Univention Configuration Registry

Der zu verwendende Repository-Server wird in die Univention Configuration Registry Variable *repository/online/server* (Seite 316) eingetragen und ist bei einer Neuinstallation auf `updates.software-univention.de` voreingestellt.

5.4.3 Richtlinienbasierte Konfiguration des Repository-Servers

Der zu verwendende Repository-Server kann auch über die Richtlinie *Repository-Server* im Univention Management Console-Modul *Rechner* festgelegt werden. In dem Auswahlfeld werden UCS-Server-Systeme angezeigt, für die ein DNS-Eintrag hinterlegt ist (siehe auch *Richtlinien* (Seite 77)).

5.4.4 Einrichtung und Aktualisierung eines lokalen Repositorys

Paketinstallationen und Updates können entweder vom Univention-Update-Server oder von einem lokal gepflegten Repository durchgeführt werden. Ein lokales Repository ist sinnvoll, wenn viele UCS-Systeme zu aktualisieren sind, da Updates in diesem Fall nur einmalig heruntergeladen werden müssen. Da Repositorys auch offline aktualisiert werden können, ermöglicht ein lokales Repository auch die Aktualisierung von UCS-Umgebungen ohne Internetanbindung.

Durch die Univention Configuration Registry Variable *local/repository* (Seite 310) kann das lokale Repository aktiviert/deaktiviert werden.

Es besteht auch die Möglichkeit lokale Repositorys zu synchronisieren, so dass beispielsweise in der Firmenzentrale ein Haupt-Repository gepflegt wird, das dann in lokale Repositorys der einzelnen Standorte synchronisiert wird.

Um ein Repository einzurichten, muss der Befehl **univention-repository-create** als Benutzer `root` aufgerufen werden.

Mit dem Tool **univention-repository-update** werden die Pakete im Repository aktualisiert. Mit **univention-repository-update net** wird das Repository mit einem angegebenen anderen Repository-Server synchronisiert. Dieser ist in der Univention Configuration Registry Variable *repository/mirror/server* (Seite 316) definiert (typischerweise `updates.software-univention.de`).

Eine Übersicht über die möglichen Optionen kann mit folgendem Befehl aufgerufen werden:

```
$ univention-repository-update -h
```

Das Repository wird im Verzeichnis `/var/lib/univention-repository/mirror/` vorgehalten.

5.5 Installation weiterer Software

Die Erstauswahl der Softwarekomponenten eines UCS-Systems erfolgt im Rahmen der Installation. Die Auswahl der Softwarekomponenten erfolgt dabei funktionsbezogen, indem etwa die Komponente *Proxy-Server* ausgewählt wird, die dann über ein Meta-Paket die eigentlichen Software-Pakete nachzieht. Der Administrator muss dazu die eigentlichen Paketnamen nicht kennen. Für weitergehende Aufgaben können aber auch einzelne Pakete gezielt installiert und entfernt werden. Bei der Installation eines Pakets werden unter Umständen Pakete mitinstalliert, die für die Funktion des angegebenen Pakets erforderlich sind, die sogenannten Paketabhängigkeiten. Alle Softwarekomponenten werden aus einem Repository geladen (siehe *Konfiguration des Repository-Servers für Updates und Paketinstallationen* (Seite 102)).

Fremdsoftware, die nicht im Debian-Paketformat vorliegt, sollte in die Verzeichnisse `/opt/` oder `/usr/local/` installiert werden. UCS-Pakete nutzen diese Verzeichnisse nicht, so dass eine saubere Trennung von UCS- und Fremdsoftware gewährleistet ist.

Um auf einem bereits installierten System nachträglich weitere Pakete zu installieren, stehen mehrere Möglichkeiten zur Verfügung.

5.5.1 Installation/Deinstallation von UCS-Komponenten im Univention App Center

Alle Softwarekomponenten, die im Univention Installer angeboten werden, können auch über das Univention App Center nachträglich installiert und entfernt werden. Dazu muss die Paket-Kategorie *UCS-Komponenten* ausgewählt werden. Weitere Hinweise zum Univention App Center finden sich in *Univention App Center* (Seite 96).

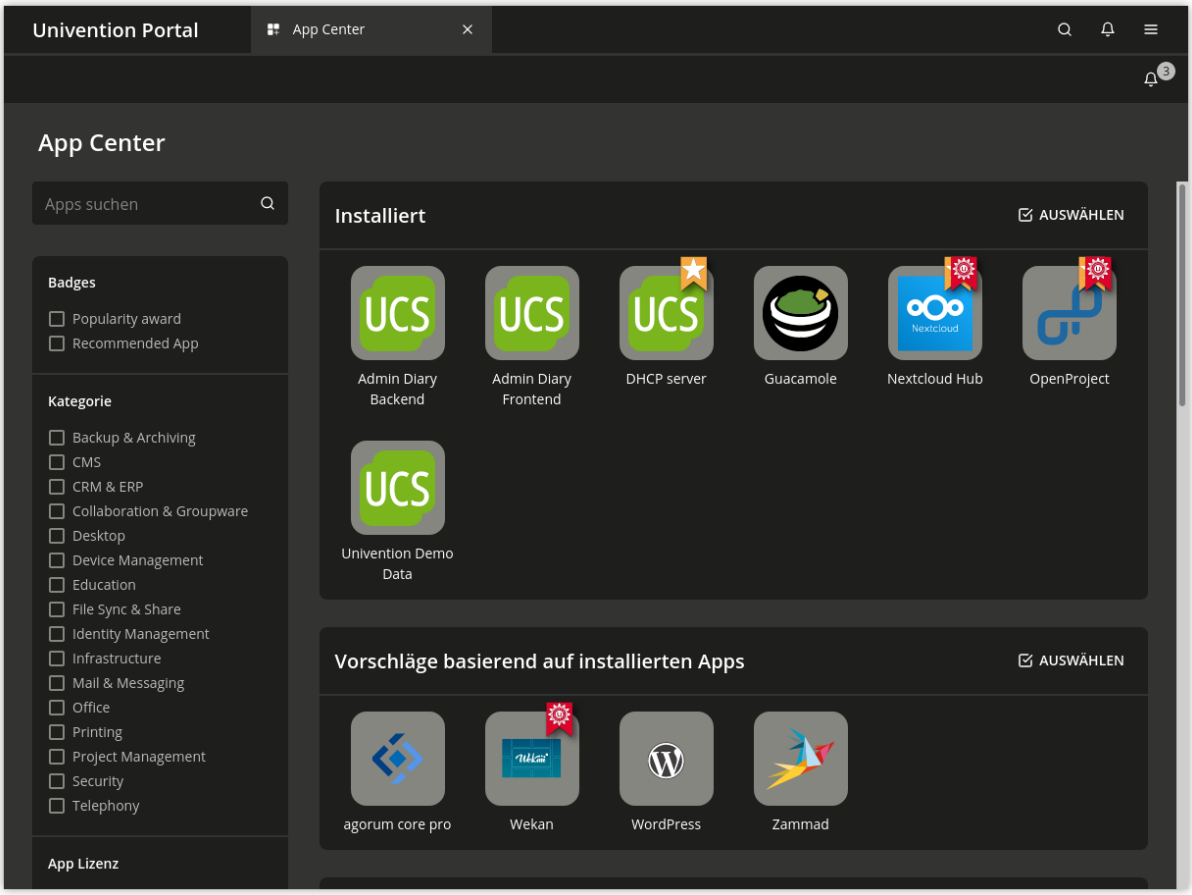


Abb. 5.6: Auswahl von UCS-Komponenten im App Center

5.5.2 Installation/Entfernung einzelner Pakete über Univention Management Console-Modul

Mit dem UMC-Modul *Paket-Verwaltung* können einzelne Softwarepakete installiert und deinstalliert werden.

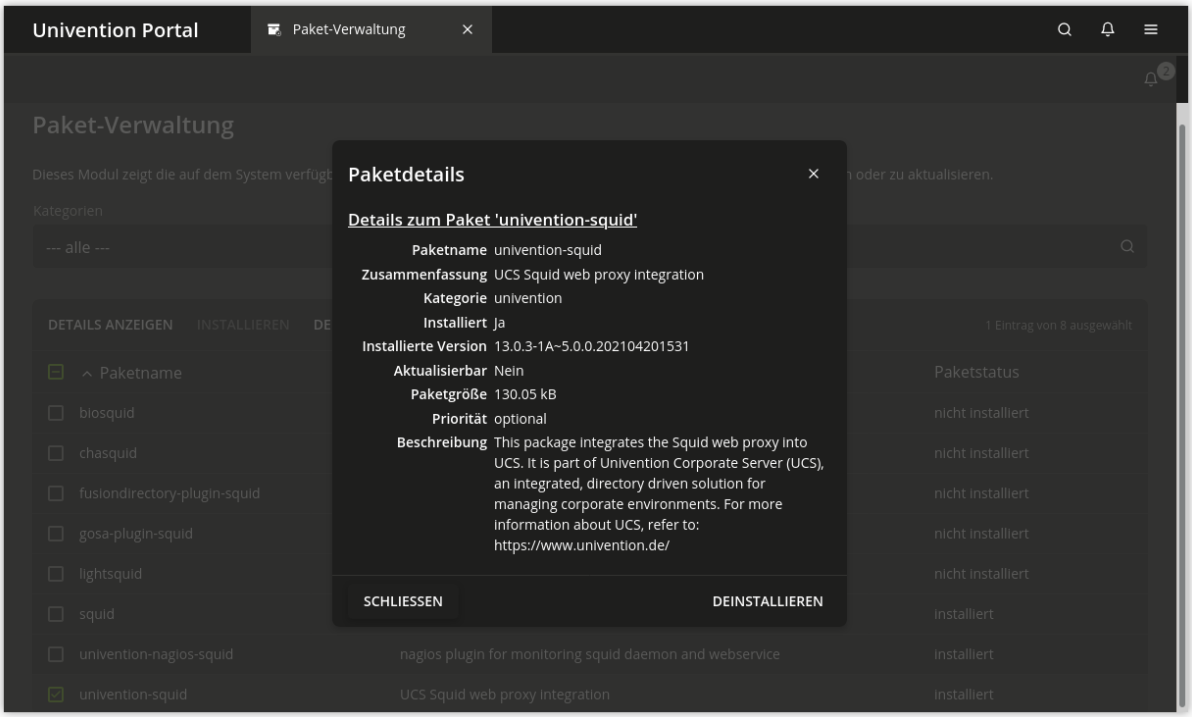


Abb. 5.7: Installation des Pakets **`univention-squid`** mittels Univention Management Console Modul *Paket-Verwaltung*

Auf der Startseite wird eine Suchmaske angezeigt in der die Paketkategorie und ein Suchfilter (Name oder Beschreibung) zur Auswahl stehen. Die Ergebnisliste besteht aus einer Tabelle mit den folgenden Spalten:

- Paketname
- Paketbeschreibung
- Installationsstatus

Durch einen Klick auf eine Zeile in der Ergebnisliste wird eine detaillierte Informationsseite zu dem Softwarepaket angezeigt, u.a. eine ausführliche Beschreibung und die Versionsnummer.

Zusätzlich werden ein oder mehrere Buttons angezeigt. Sie haben die folgenden Bedeutungen:

Installieren
: wird angezeigt, falls das Softwarepaket noch nicht installiert ist.

Deinstallieren
: wird angezeigt, falls das Paket installiert ist.

Aktualisieren
: wird angezeigt, falls das Softwarepaket bereits installiert, aber nicht aktuell ist.

Schließen
: kann verwendet werden, um zur vorherigen Suchanfrage zurück zu kehren.

5.5.3 Installation/Deinstallation von einzelnen Paketen auf der Kommandozeile

Die folgenden Schritte müssen mit `root`-Rechten durchgeführt werden.

Die Installation einzelner Pakete erfolgt mit dem Kommando

```
$ univention-install PACKAGENAME
```

Pakete können mit dem folgenden Befehl entfernt werden:

```
$ univention-remove PACKAGENAME
```

Wenn der Name eines Pakets nicht bekannt ist, kann mit dem Kommando **`apt-cache search`** nach Paketen gesucht werden. Als Aufrufparameter können Teile des Namens oder Wörter, die in der Beschreibung eines Paketes vorkommen, angegeben werden, z.B.

```
$ apt-cache search fax
```

5.5.4 Hook Skripte für Administratoren

Benutzerdefinierte Skripte können nach jeder Installation, Aktualisierung oder Deinstallation von Apps ausgeführt werden. Solche Skripte erlauben die Automatisierung wiederkehrender administrativer Aufgaben.

Um von dieser Eigenschaft Gebrauch zu machen, können Skripte in einem der folgenden Verzeichnisse abgelegt werden. Wenn ein solches Verzeichnis noch nicht existiert, kann es manuell angelegt werden.

- `/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-install.d/`
- `/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-upgrade.d/`
- `/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-remove.d/`

Wobei `{appid}` der Name einer App ist, für welche die Skripte ausgeführt werden sollen.

Dateinamen dürfen nur aus Kleinbuchstaben und Zahlen bestehen (`^[a-z0-9]+$`). Außerdem müssen die Dateien als ausführbar markiert sein (**`chmod +x [Dateiname]`**) denn sie werden intern von **`run-parts`** aufgerufen. Daher kann mit **`run-parts --test [Verzeichnis]`** getestet werden, ob und welche Dateien ausgeführt werden würden. Weitere Informationen können der Manpage entnommen werden mit **`man run-parts`**.

Die `/var/log/univention/appcenter.log` enthält mögliche Fehler bei der Ausführung der Skripte und weitere Hinweise.

5.5.5 Richtlinienbasierte Installation/Deinstallation von einzelnen Paketen über Paketlisten

Mit Paketlisten kann richtlinienbasiert Software installiert und entfernt werden. Dadurch lassen sich auch große Stückzahlen an Rechnersystemen zentral mit neuer Software versehen.

Jede Systemrolle verfügt über eine eigenen Paket-Richtlinien-Typ.

Paketrichtlinien werden im UMC-Modul *Richtlinien* mit dem Objekttyp *Richtlinie: Pakete + Systemrolle* verwaltet.

Tab. 5.1: Reiter *Allgemein*

Attribut	Beschreibung
Name	Ein eindeutiger Name für diese Paketliste, z.B. *Standort-Server*.
Pakete Installationsliste	Eine Liste zu installierender Pakete.
Pakete Deinstallationsliste	Eine Liste zu entfernender Pakete.

Die in einer Paketliste definierten Softwarepakete werden zu dem in der *Paketpflege*-Richtlinie definierten Zeitpunkt (zur Konfiguration siehe *Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie* (Seite 107)) installiert oder deinstalliert.

Die in den Pakete-Richtlinien zuordbaren Softwarepakete werden ebenfalls im LDAP registriert.

5.6 Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie

Mit einer *Paketpflege*-Richtlinie (siehe auch *Richtlinien* (Seite 77)) in den UMC-Modulen zur Rechner- und Domänenverwaltung kann ein Zeitpunkt vorgegeben werden, an dem die folgenden Schritte durchgeführt werden:

- Prüfung auf verfügbare und zu installierende Release-Updates (siehe *Aktualisierung von Systemen über eine Rechner-Richtlinie* (Seite 101)) und gegebenenfalls Installation
- Installation/Deinstallation von Paketlisten (siehe *Richtlinienbasierte Installation/Deinstallation von einzelnen Paketen über Paketlisten* (Seite 106))
- Installation verfügbarer Errata-Updates

Alternativ können die Aktualisierungen auch beim Systemstart oder beim Herunterfahren des Systems erfolgen.

Tab. 5.2: Reiter *Allgemein*

Attribut	Beschreibung
Paketpflege durchführen nach Hochfahren des Systems	Falls diese Option aktiviert ist, werden die Aktualisierungsschritte während des Startvorgangs des Rechners durchgeführt.
Paketpflege durchführen vor Herunterfahren des Systems	Falls diese Option aktiviert ist, werden die Aktualisierungsschritte beim Herunterfahren des Rechners durchgeführt.
Cron Einstellung benutzen	Wird dieses Feld aktiviert, kann über die Felder *Monat*, *Wochentag*, *Tag*, *Stunde* und *Minute* ein genauer Zeitpunkt angegeben werden, an dem die Aktualisierungsschritte durchgeführt werden sollen.
Nach Paketpflege neu starten	Diese Option ermöglicht es, nach Release-Aktualisierungen optional einen automatischen Neustart des Systems durchzuführen, entweder direkt oder nach dem angegebenen Zeitintervall in Stunden.

5.7 Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor

Der Software-Monitor ist eine Datenbank, in der Informationen über die auf UCS-Systemen installierten Softwarepakete aufgezeichnet werden. Durch diese Datenbank kann sich ein Administrator einen Überblick verschaffen, welche Release- und Paketversionen auf den Systemen der Domäne installiert sind und diese Informationen bei der schrittweisen Aktualisierung einer UCS-Domäne nutzen und Installations-Probleme erkennen.

Der Software-Monitor kann mit der Applikation *Software-Installationsmonitor* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **`univention-pkgdb`** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

UCS-Systeme aktualisieren ihre Einträge bei der Installation, Entfernung und Aktualisierung von Software automatisch. Das System, auf dem der Software-Monitor betrieben wird, wird dabei durch den DNS-Service-Record `_pkgdb._tcp` lokalisiert.

Der Software-Monitor bringt sein eigenes UMC-Modul *Software-Monitor* mit. Folgende Funktionen stehen zur Verfügung:

Systeme
erlaubt die Suche nach den installierten Versionsständen von UCS-Systemen. Es kann nach Systemnamen, UCS-Versionen und Systemrollen gesucht werden.

Pakete
ermöglicht die Suche in den von der Paketstatusdatenbank erfassten Installationsdaten. Neben der Suche nach *Paketnamen* gibt es auch die folgenden Suchmöglichkeiten zu den Installationszuständen von Paketen:

Auswahlstatus
Der *Auswahlstatus* beeinflusst das Verhalten bei der Aktualisierung eines Pakets. Durch `Install` wird ein Paket zur Installation ausgewählt. Ist ein Paket auf `Hold` konfiguriert, so wird es von weiterer Aktualisierung ausgenommen. Es existieren zwei Möglichkeiten ein Paket zu deinstallieren: Ein mit `De-Install` entferntes Paket hält lokal erzeugte Konfigurations-Daten weiterhin vor, während ein mit `Purge` entferntes Paket komplett gelöscht wird.

Installationsstatus
Der *Installationsstatus* beschreibt den Status eines installierten Pakets im Hinblick auf kommende Aktualisierungen. Der Normalfall ist `Ok`, was dazu führt, dass ein Paket bei Vorhandensein einer aktuelleren Version aktualisiert würde. Ist ein Paket auf `Hold` konfiguriert, so wird es von der Aktualisierung ausgenommen.

Paketstatus
Der *Paketstatus* beschreibt den Zustand eines eingerichteten Pakets. Der Normalfall ist `Installed` für installierte und `ConfigFiles` für entfernte Pakete, alle übrigen Zustände entstehen, wenn die Installation des Pakets in verschiedenen Phasen abgebrochen wurde.

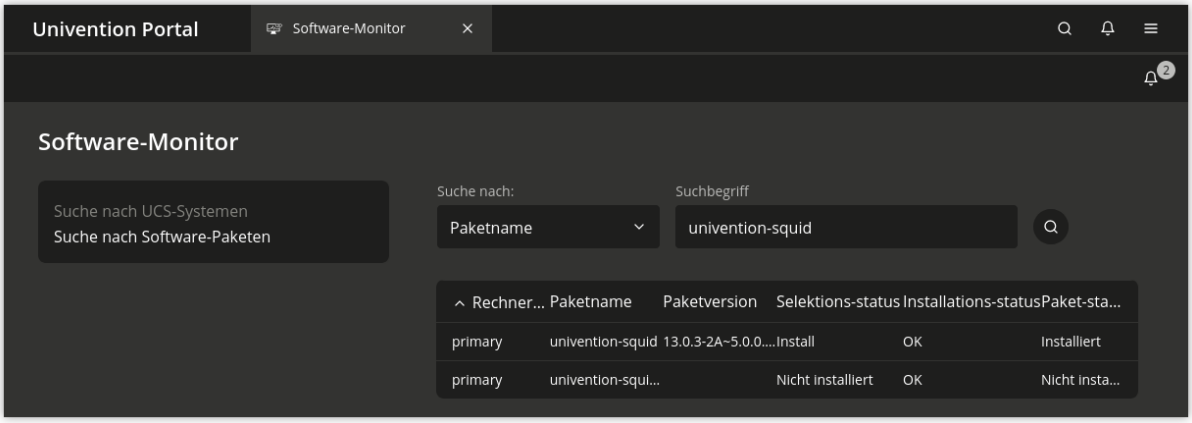


Abb. 5.8: Suche nach Paketen im Software-Monitor

Wenn verhindert werden soll, dass UCS-Systeme Installationsvorgänge im Software-Monitor aufzeichnen, etwa weil keine Netzwerkverbindung zur Datenbank besteht, kann dies durch Setzen der Univention Configuration Registry Variable *pkgdb/scan* (Seite 315) auf `no` abgeschaltet werden.

Wenn die Aufzeichnungen danach wieder aktiviert werden, muss das Kommando **`univention-pkgdb-scan`** ausgeführt werden, damit die in der Zwischenzeit installierten Paketversionen in die Datenbank übernommen werden.

Mit dem folgenden Befehl kann der Programmbestand eines Systems wieder aus der Datenbank entfernt werden:

```
$ univention-pkgdb-scan --remove-system [HOSTNAME]
```

KAPITEL 6

Benutzerverwaltung

UCS integriert ein zentrales Identity-Management. Alle Benutzerinformationen werden in UCS zentral über das UMC-Modul *Benutzer* verwaltet und im LDAP-Verzeichnisdienst gespeichert.

Bemerkung: Die Benutzerverwaltung ist Teil von Univention Nubus in der *Directory Manager* Komponente. Weitere Informationen zu Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 2)

Alle in die Domäne integrierten Dienste greifen dabei auf die zentralen Kontoinformationen zu, d.h. für die Benutzeranmeldung an einem Windows-Client wird die gleiche Benutzerkennung und das gleiche Passwort verwendet wie etwa bei der Anmeldung am IMAP-Server.

Die domänenweite Verwaltung von Benutzerdaten verringert den administrativen Aufwand, da Änderungen nicht auf verschiedenen Einzelsystemen nachkonfiguriert werden müssen. Darüber hinaus vermeidet dies Folgefehler, die sich durch Inkonsistenzen zwischen den einzelnen Datenbeständen ergeben können.

Arten von Benutzerkonten

In UCS gibt es drei unterschiedliche Arten von Benutzerkonten:

1. *Vollwertige Benutzerkonten*: Normale, vollwertige Benutzerkonten haben sämtliche verfügbaren Eigenschaften. Diese Benutzer können sich an UCS- oder Windows-Systemen anmelden und je nach Konfiguration auch an den installierten Apps. Die Benutzer können über das UMC-Modul *Benutzer* (siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110)) administriert werden.
2. *Adressbucheinträge*: Adressbucheinträge können für die Pflege von internen oder externen Kontaktinformationen verwendet werden. Diese Kontakte können sich nicht an UCS- oder Windows-Systemen anmelden. Adressbucheinträge können über das UMC-Modul *Kontakte* verwaltet werden.
3. *Einfaches Authentisierungskonto*: Mit einem einfachen Authentisierungskonto wird ein Benutzer-Objekt angelegt, welches ausschließlich einen Benutzernamen und ein Passwort hat. Mit diesem Konto ist ausschließlich eine Authentisierung gegen den LDAP-Verzeichnisdienst möglich, aber keine Anmeldung an UCS- oder Windows-Systemen. Einfache Authentisierungskonten können über das UMC-Modul *LDAP-Verzeichnis* (siehe *LDAP-Verzeichnis-Browser* (Seite 76)) erstellt werden.

Empfehlung zur Definition von Benutzernamen

Ein sehr wichtiges und erforderliches Attribut für Benutzerkonten ist der Benutzername. Um Konflikte mit den verschiedenen Werkzeugen zu vermeiden, die Benutzerkonten in UCS verarbeiten, berücksichtigen Sie die folgenden Empfehlungen für die Definition von Benutzernamen:

- Verwenden Sie für Benutzernamen nur Kleinbuchstaben (`a-z`), Ziffern (`0-9`) und den Bindestrich (`-`) aus dem ASCII-Zeichensatz.
- Der Benutzername beginnt mit einem Kleinbuchstaben aus dem ASCII-Zeichensatz. Der Bindestrich als letztes Zeichen ist nicht erlaubt.
- In UCS hat der Benutzername eine Länge von mindestens 4 und höchstens 20 Zeichen.

Die Empfehlung ergibt den folgenden regulären Ausdruck: `^[a-z][a-z0-9-]{2,18}[a-z0-9]$`.

Neben der Empfehlung enthalten Benutzernamen in der Praxis auch Unterstriche (_) und ASCII-Großbuchstaben. Betrachten Sie die Empfehlung als Richtlinie und nicht als harte Regel und bedenken Sie mögliche Nebenwirkungen, wenn Sie Benutzernamen außerhalb der Empfehlung definieren.

6.1 Verwaltung von Benutzern über Univention Management Console Modul

Dieser Abschnitt beschreibt die Benutzerverwaltung über das UMC-Modul *Benutzer*.

6.1.1 Assistent zur Benutzererstellung

Zum Anlegen von Benutzern können Administratoren den vereinfachten Assistenten verwenden, wie in den folgenden Abbildungen dargestellt.

Sie öffnen den Assistenten, indem Sie im Modul *Benutzer* auf die Schaltfläche *Hinzufügen* klicken. Auf der ersten Seite in *Neuen Benutzer hinzufügen* wählen Sie den *Container* aus, in dem Sie das Benutzerobjekt unterbringen möchten, und ob Sie ein Benutzerkonto mit einer Vorlage erstellen möchten.

Wenn Sie auf *Weiter* klicken, sehen Sie die Seite in Abb. 6.1.

Mit *Weiter* zeigt das UMC-Modul *Benutzer* die dritte Seite wie in Abb. 6.2 an, wo Sie das Anfangspasswort festlegen können.

Alternativ kann der Benutzer das initiale Passwort selbst setzen, wenn in der UCS-Domäne die App **`Self Service`** installiert ist. Um dem Benutzer die Möglichkeit zu geben, das initiale Passwort selbst zu setzen, müssen Sie eine externe E-Mail-Adresse definieren.

Öffnen Sie zum Definieren einer externen E-Mailadresse in den *Erweiterten* Benutzerkontoeinstellungen die Registerkarte *Kontakt* und geben Sie eine externe E-Mail-Adresse in das Feld *E-Mail-Adresse* ein. Die Self Service App sendet eine E-Mail an die externe E-Mail-Adresse des Benutzers mit einem Link und einem Token. Über den Link kann der Benutzer sein initiales Passwort festlegen und das Benutzerkonto freischalten. Weitere Informationen finden Sie unter *Passwort-Verwaltung über Self Service App* (Seite 124).

Das Modul *Benutzer* zeigt standardmäßig einen vereinfachten Assistenten zum Anlegen eines Benutzers. Der Assistent fragt nur die wichtigsten Einstellungen ab. Um alle Attribute des Benutzerkontos wie in Abb. 6.4 zu sehen, klicken Sie im Assistenten auf *Erweitert*.

Sie können den vereinfachten Assistenten deaktivieren, indem Sie die *`directory/manager/web/modules/users/user/wizard/disabled`* (Seite 305) auf `true` setzen und den **`univention-management-console-server`** neu starten.

Wenn Sie die primäre E-Mail-Adresse des Benutzers im vereinfachten Assistenten festlegen möchten, können Sie das Feld aktivieren, indem Sie die Univention Configuration Registry Variable `directory/manager/web/modules/users/user/properties/mailPrimaryAddress/required` auf `true` setzen und den

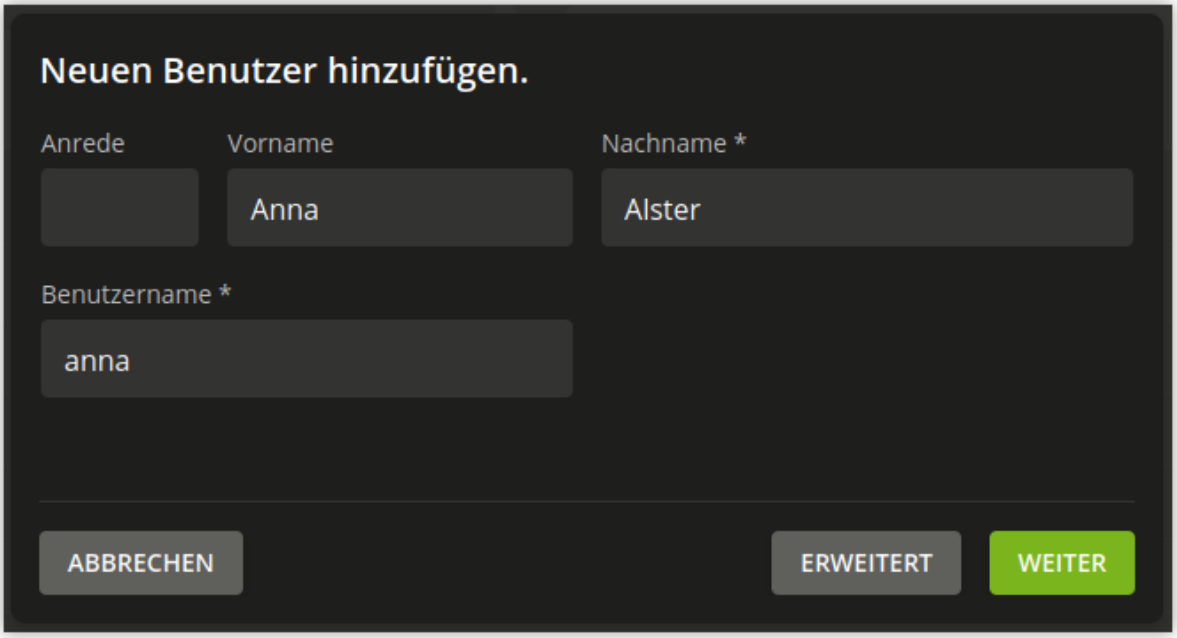


Abb. 6.1: Anlegen eines Benutzers im UMC-Modul *Benutzer*

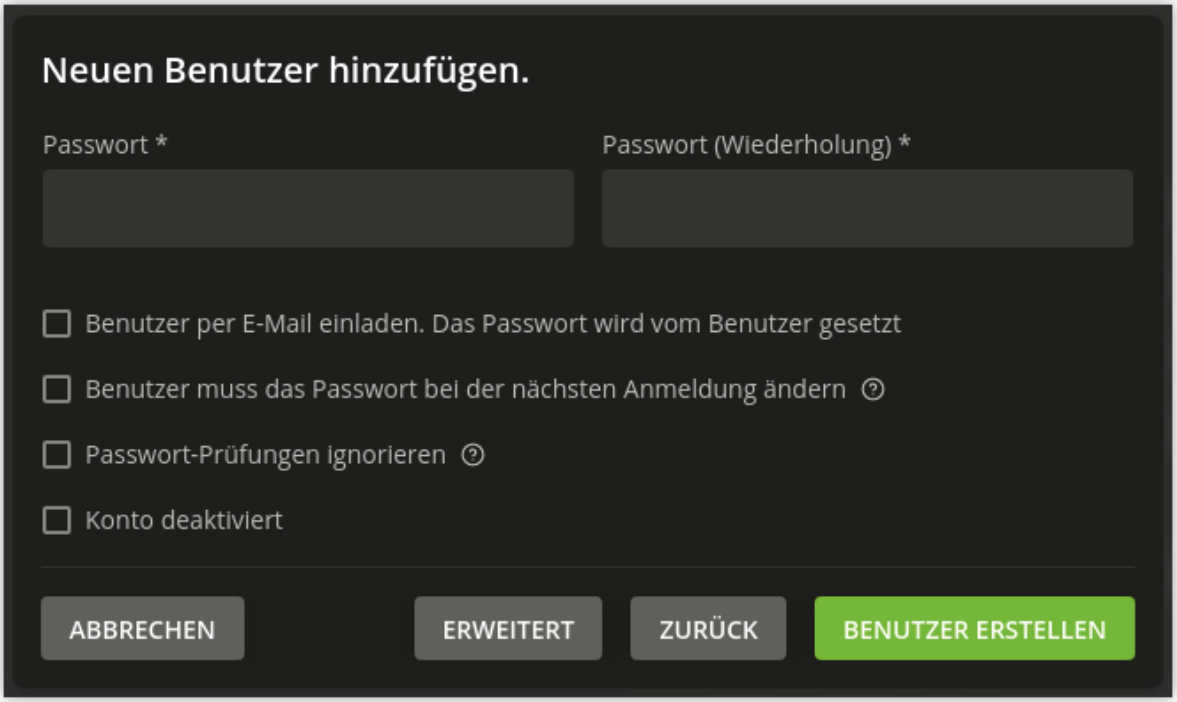


Abb. 6.2: Passwortvergabe für einen Benutzer

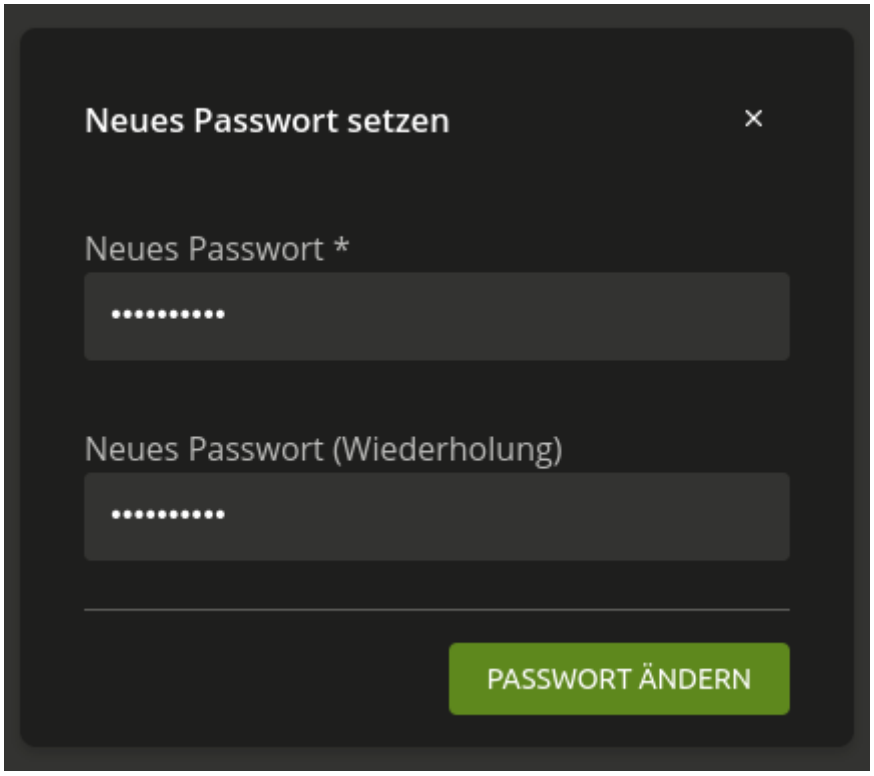


Abb. 6.3: Initiales Benutzerpasswort

univention-management-console-server neu starten. Die zweite Seite des Assistenten fragt dann nach der primären E-Mail-Adresse des Benutzers, wie in Abb. 6.5 gezeigt.

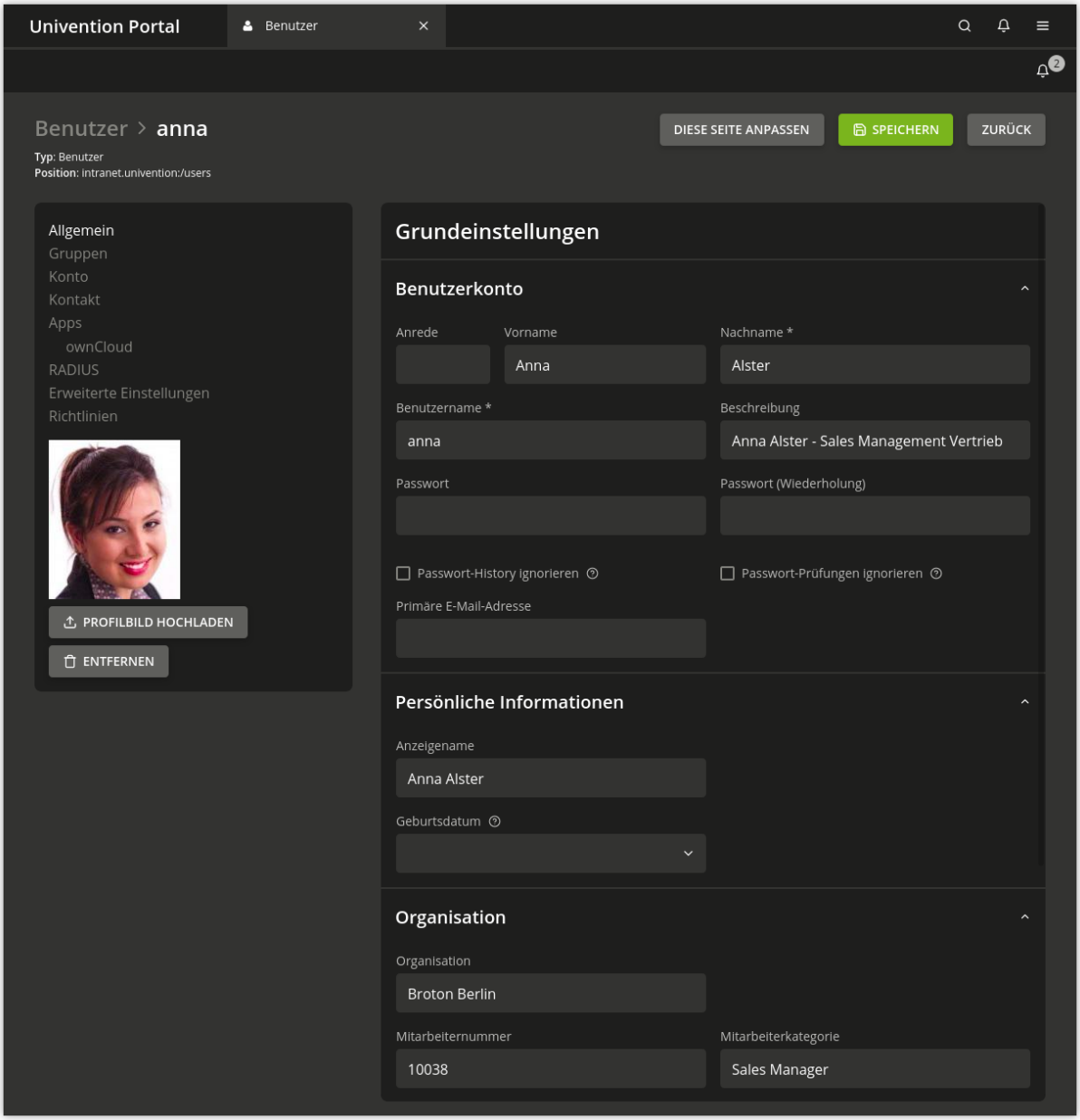


Abb. 6.4: Erweiterte Benutzeransicht

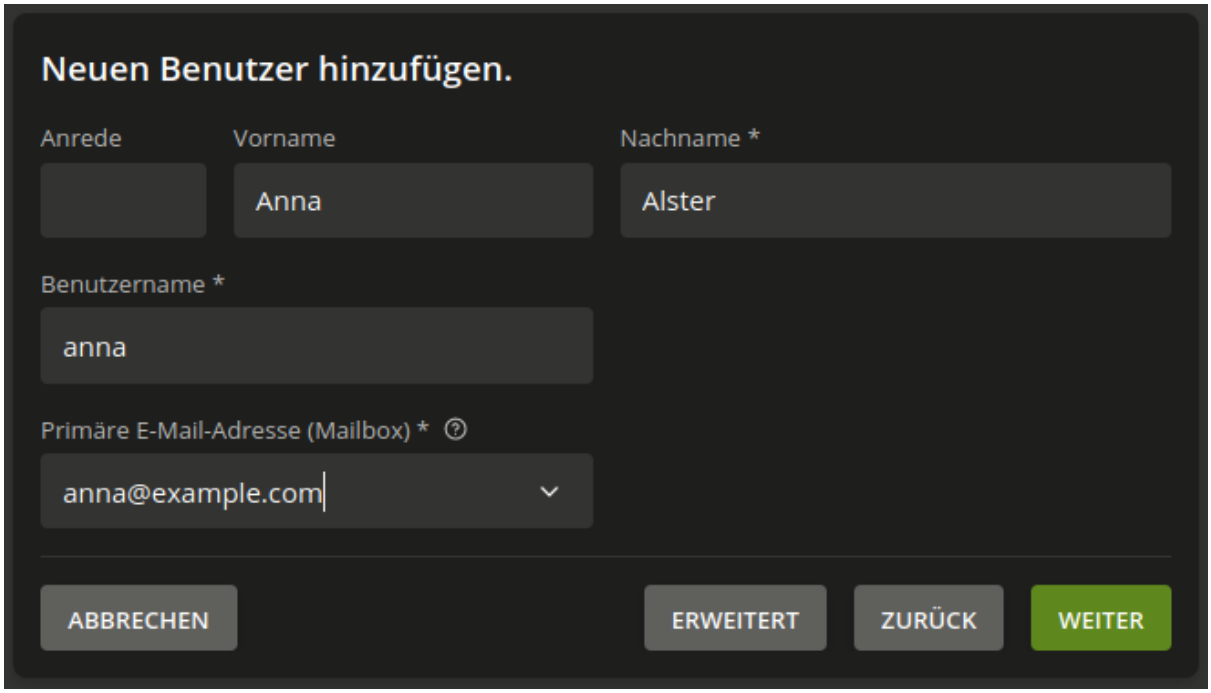


Abb. 6.5: Die primäre E-Mail-Adresse des Benutzers muss im Assistenten festgelegt werden

6.1.2 Modul Benutzerverwaltung - Reiter Allgemein

Tab. 6.1: Reiter *Allgemein*

Attribut	Beschreibung
Anrede	Die Anrede des Benutzers kann hier eingegeben werden.
Vorname	Hier wird der Vorname des Benutzers eingetragen.
Nachname	Hier wird der Nachname des Benutzers angegeben.
Benutzername	Mit diesem Namen meldet sich der Benutzer am System an. Für empfohlene Zeichen für einen Benutzernamen, siehe *Empfehlung zur Definition von Benutzernamen* (Seite 109). Um die Kompatibilität mit Nicht-UCS-Systemen zu gewährleisten, wird das Anlegen von Benutzern, die sich lediglich in der Groß- und Kleinschreibung unterscheiden, verhindert. Wenn beispielsweise der Benutzername `meier` bereits existiert, wird der Benutzername `Meier` nicht mehr zugelassen. In der Grundeinstellung kann kein Benutzer mit dem Namen einer existierenden Gruppe angelegt werden. Wird die Univention Configuration Registry Variable `directory/manager/user_group/uniqueness` (Seite 305) auf `false` gesetzt, wird diese Prüfung aufgehoben.
Beschreibung	Hier kann eine beliebige Beschreibung für den Benutzer eingetragen werden.
Passwort	Hier wird das Passwort des Benutzers eingegeben.
Passwort (Wiederholung)	Um Tippfehler auszuschließen wird das Passwort des Benutzers erneut eingegeben.
Passworthistorie ignorieren	Durch die Aktivierung dieses Auswahlkästchens wird die Passworthistorie für diesen Benutzer und für diese Passwortänderung außer Kraft gesetzt. Dadurch kann dem Benutzer mit dieser Änderung ein bereits verwendetes Passwort zugewiesen werden. Weitere Hinweise zur Passwortverwaltung finden sich in *Verwaltung der Benutzerpasswörter* (Seite 120).
Passwort-Prüfungen ignorieren	Wird diese Option aktiviert, wird die Prüfung der Passwortlänge und -qualität für diesen Benutzer und für diese Passwortänderung außer Kraft gesetzt. Dadurch kann dem Benutzer mit dieser Änderung z.B. ein kürzeres Passwort zugewiesen werden, als in der Mindestlänge vorgegeben ist. Weitere Hinweise zur Passwortverwaltung finden sich in *Verwaltung der Benutzerpasswörter* (Seite 120).
Primäre E-Mail-Adresse (Mailbox)	Hier wird die E-Mail-Adresse des Benutzers eingetragen, siehe *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 272).
Anzeigename	Der Anzeigename wird automatisch aus Vor- und Nachname gebildet. In der Regel muss er nicht angepasst werden. Der Anzeigename wird u.a. in der Synchronisation mit Active Directory und Samba/AD verwendet.
Geburtsdatum	In diesem Feld kann das Geburtsdatum des Benutzers gespeichert werden.
Organisation	Die Organisation/das Unternehmen, dem der Benutzer angehört, wird in diesem Feld eingetragen.
Mitarbeiternummer	Die Mitarbeiter- oder Personalnummer kann in dieses Feld eingetragen werden.
Mitarbeiterkategorie	Hier kann die Kategorie des Mitarbeiters festgelegt werden.
Vorgesetzter	Der Vorgesetzte des Benutzers kann hier ausgewählt werden.
Bild des Benutzers (JPEG-Format)	Über diese Maske kann ein Bild des Benutzers im JPEG-Format im LDAP hinterlegt werden. Standardmäßig ist die Dateigröße auf 512 Kilobyte limitiert.

6.1.3 Modul Benutzerverwaltung - Reiter Gruppen

Tab. 6.2: Reiter *Gruppen*

Attribut	Beschreibung
Primäre Gruppe	In dieser Auswahlliste kann die primäre Gruppe für den Benutzer festgelegt werden. Zur Auswahl stehen alle in der Domäne eingetragenen Gruppen. Standardmäßig ist die Gruppe `Domain Users` als Vorgabe eingestellt.
Gruppen	Hier können weitere Gruppenzugehörigkeiten des Benutzers neben der primären Gruppe eingestellt werden.

6.1.4 Modul Benutzerverwaltung - Reiter Konto

Tab. 6.3: Reiter *Konto*

Attribut	Beschreibung
Konto ist deaktiviert	Mir dem Auswahlkästchen *Konto ist deaktiviert* kann das Benutzerkonto deaktiviert werden. Wenn das Auswahlkästchen gesetzt ist, kann sich der Benutzer nicht am System anmelden. Das betrifft alle Methoden für die Authentifikation. Ein typischer Anwendungsfall ist ein Benutzer, der das Unternehmen verlassen hat. Eine Kontodeaktivierung kann in einer heterogenen Umgebung gegebenenfalls auch durch externe Tools ausgelöst werden.
Konto-Ablaufdatum	In diesem Eingabefeld wird ein Datum vorgegeben, an dem das Konto automatisch gesperrt wird. Dies ist sinnvoll für zeitlich befristete Benutzerkonten, z.B. für Praktikanten. Wenn das Datum entfernt oder ein anderes, zukünftiges Datum eingetragen wird, kann sich der Benutzer wieder anmelden.
Passwort bei der nächsten Anmeldung ändern	Wenn dieses Auswahlkästchen aktiviert ist, muss der Benutzer bei der nächsten Anmeldung an der Domäne sein Passwort ändern.
Passwortablaufdatum	Wenn das Passwort zu einem bestimmten Datum abläuft, wird dieses Datum in diesem Eingabefeld angezeigt. Das Eingabefeld ist nicht direkt änderbar, siehe *Verwaltung der Benutzerpasswörter* (Seite 120). Ist ein Passwortablaufintervall definiert, wird das Passwortablaufdatum bei Passwortänderungen automatisch angepasst. Wird kein *Passwortablaufdatum* gesetzt, werden vielleicht bestehende frühere Ablaufdaten entfernt.
Aussperrung zurücksetzen	Wenn das Benutzerkonto aus Sicherheitsgründen automatisch gesperrt worden ist, meist weil ein Benutzer sein Passwort zu oft fehlerhaft eingegeben hat, kann dieses Auswahlkästchen dazu verwendet werden, um das Konto manuell schon vor Ablauf der Sperrzeit zu entsperren. Eine temporäre Aussperrung kann auftreten, wenn ein Administrator eine entsprechende domänenweite Einstellung definiert hat. Es gibt drei unterschiedliche Mechanismen, die eine Aussperrung auslösen können, falls sie konfiguriert wurden: • Fehlgeschlagene Authentifikation per PAM an einem UCS-Server (siehe *Automatisches Sperren von Benutzern nach fehlgeschlagenen Anmeldungen* (Seite 132)). • Fehlgeschlagene Authentifikation per LDAP (falls das Overlay-Modul `ppolicy` aktiviert und konfiguriert wurde). • Fehlgeschlagene Authentifikation per Samba/AD (falls die Samba domain `passwordsettings` konfiguriert wurden).
Aussperrung endet	Wenn das Benutzerkonto aus Sicherheitsgründen automatisch gesperrt worden ist, meist weil ein Benutzer sein Passwort zu oft fehlerhaft eingegeben hat, zeigt dieses Feld den Zeitpunkt an, ab dem das Konto regulär automatisch entsperrt wird.
Aktivierungsdatum	Wenn ein Benutzerkonto erst an einem bestimmten, zukünftigen Datum aktiviert werden soll, kann hier das Datum eingestellt werden. Ein Cron-Job prüft periodisch, ob Benutzerkonten aktiviert werden müssen. Per Voreinstellung geschieht das alle 15 Minuten. Wird hier ein Datum eingestellt, das in der Zukunft liegt, dann wird beim Speichern automatisch auch das Konto als deaktiviert markiert.
Laufwerk für das Windows-Heimatverzeichnis	Wenn das Windows-Heimatverzeichnis bei diesem Benutzer auf einem anderen Windows-Laufwerk erscheinen soll, als in der Samba-Konfiguration vorgegeben, so kann hier ein Laufwerksbuchstabe eingetragen werden, z.B. `M:`.
Windows-Heimatverzeichnis	Hier wird der Pfad zu dem Verzeichnis angegeben, das als Windows-Heimatverzeichnis für den Benutzer dienen soll, z.B. `\ucs-file-servermeier`.
Anmeldeskript	Hier wird das benutzerspezifische Anmeldeskript relativ zur Netlogon-Freigabe eingetragen, z.B. `user.bat`.
Profilverzeichnis	Das Profilverzeichnis für den Benutzer kann hier angegeben werden, e.g. `\ucs-file-serveruserprofile`.
Relative ID	Die relative ID (RID) ist der lokale Teil der SID-Domänenkennung. Wenn ein Benutzer eine bestimmte RID erhalten soll, so kann diese hier eingetragen werden. Wenn keine RID eingetragen wird, so wird automatisch die nächste freie RID verwendet. Die RID kann nachträglich nicht geändert werden, es sind gan-

6.1.5 Modul Benutzerverwaltung - Reiter Kontakt

Tab. 6.4: Reiter *Kontakt*

Attribut	Beschreibung
E-Mail-Adresse(n)	Hier können weitere E-Mail-Adressen hinterlegt werden. Diese werden nicht vom Mailserver ausgewertet. Die Werte werden im LDAP-Attribut `mail` gespeichert. Die meisten Adressbuch-Applikationen suchen im LDAP nach diesem Attribut.
Telefonnummer(n)	Dieses Feld beinhaltet die geschäftlichen Telefonnummern des Benutzers.
Raumnummer	Die Raumnummer des Benutzers.
Abteilungsnummer	Hier kann die Abteilungsnummer des Mitarbeiters angegeben werden.
Straße	Die Straße und die Hausnummer der Geschäftsadresse des Benutzers kann hier eingetragen werden.
Postleitzahl	Dieses Feld beinhaltet die Postleitzahl der Geschäftsadresse des Benutzers.
Stadt	Dieses Feld beinhaltet die Stadt der Geschäftsadresse des Benutzers.
Telefonnummer(n) Festnetz	Die privaten Festnetznummern können hier angegeben werden.
Telefonnummer(n) Mobil	Hier werden die privaten Mobilfunknummern des Benutzers eingetragen.
Rufnummer(n) Pager	Pager-Rufnummern werden in diesem Feld angegeben.
Private Adresse	Eine oder mehrere private Postadressen des Benutzers können in diesem Feld angegeben werden.

6.1.6 Modul Benutzerverwaltung - Reiter Mail

Diese Karteikarte wird in den erweiterten Einstellungen angezeigt.

Die Einstellungen sind in *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 272) beschrieben.

6.1.7 Modul Benutzerverwaltung - Reiter Optionen

Tab. 6.5: Reiter *(Optionen)*

Attribut	Beschreibung
Public Key Infrastruktur-Konto	Wenn dieses Auswahlkästchen nicht markiert ist, erhält der Benutzer die Objektklasse `pkiUser` nicht.

6.2 Benutzeraktivierung für Apps

Viele Apps aus dem App Center sind mit dem zentralen Identity Management in UCS verknüpft. Dadurch können Systemadministratoren die Benutzer für Apps aktivieren. In manchen Fällen können noch weitere App spezifische Einstellungen für den Benutzer vorgenommen werden. Das ist abhängig von der App und wie diese das Identity Management nutzt.

Sobald eine App in der UCS-Umgebung installiert ist, die die Benutzeraktivierung verwendet, erscheint sie mit Logo im Reiter *Apps* des Benutzers im UMC-Modul *Benutzer*. Mit einem Haken in der Checkbox wird der Benutzer für die App aktiviert. Wenn noch weitere Einstellungen für die Berechtigung gemacht werden können, erscheint ein zusätzlicher Reiter mit dem Namen der App, um diese Parameter zu setzen. Die App Aktivierung und die Parameter werden am Benutzerobjekt im LDAP-Verzeichnisdienst von UCS gespeichert.

Um einem Benutzer die Berechtigung zur Nutzung einer App wieder zu entziehen, genügt es, den Haken aus Checkbox zu entfernen.

Wenn die App deinstalliert wird, wird die Checkbox der Benutzeraktivierung für die App vom Reiter *Apps* des Benutzers im UMC-Modul entfernt.

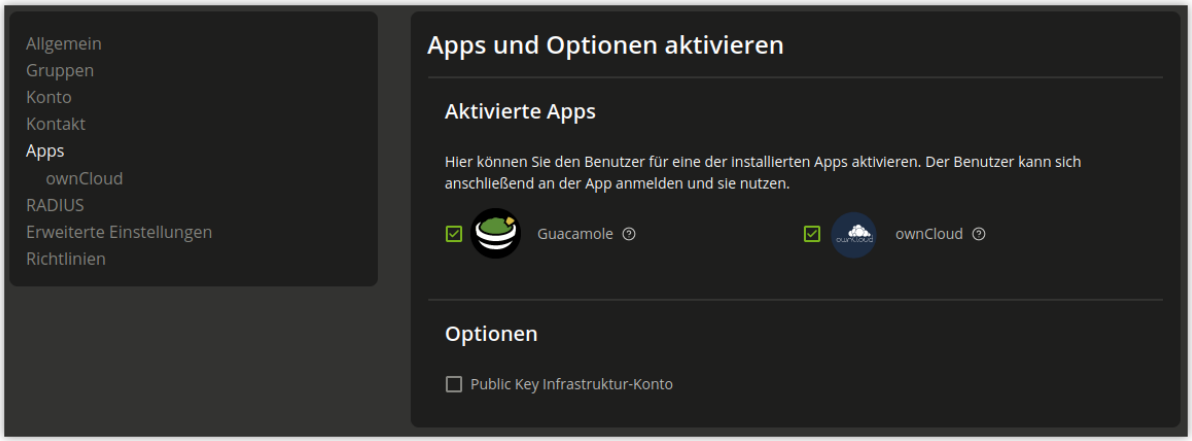


Abb. 6.6: Benutzeraktivierung für installierte Apps

6.3 Verwaltung der Benutzerpasswörter

Den meisten Internetnutzern fällt es schwer, das richtige Passwort zu wählen. Das Passwort ist der Schlüssel zum Zugriff auf Benutzerkonten, auch in einer UCS-Domäne. Schwer zu erratende Passwörter und regelmäßiger Wechsel der Passwörter sind ein wesentliches Element der Systemsicherheit einer UCS-Domäne. Um zu verhindern, dass Benutzer zu einfache Passwörter wählen, können Administratoren mehrere Eigenschaften in einer *Passwortrichtlinie* konfigurieren.

Dieser Abschnitt beschreibt, wie Sie Passwortrichtlinien definieren, z. B. eine Mindestlänge des Passworts und ein Zeitintervall für den Ablauf. UCS wendet die Passwortrichtlinie an, wenn Benutzer ihre Passwörter ändern.

UCS speichert das Benutzerpasswort für jeden Benutzer als Hash in verschiedenen Attributen des entsprechenden LDAP-Objekts des Benutzerkontos:

`krb5Key`
: speichert das Kerberos-Passwort.

`userPassword`
: speichert das Unix-Passwort. Andere Linux Distributionen speichern es in `/etc/shadow`.

`sambaNTPassword`
: speichert den von Samba verwendeten NT-Passwort-Hash.

Siehe auch:

Sichere Passwörter erstellen[24] **von Bundesamt für Sicherheit in der Informationstechnik**
: für weitere Informationen und Tipps zur Erstellung eines sicheren und guten Passworts.

6.3.1 Arten von Passwortrichtlinien

UCS verfügt über mehrere Arten von Kennwortrichtlinieneinstellungen, die in diesem Abschnitt beschrieben sind. Welche Richtlinie gilt, hängt davon ab, wer die Passwortänderung durchführt und ob in der UCS-Domäne Samba über die App **`Active Directory Domain Controller`** installiert ist.

Passwortrichtlinie in UDM
: Die *Passwortrichtlinie* ist eine UDM Richtlinie, die für die Änderung von Benutzerpasswörtern durch UMC-Module gilt, die ihrerseits UDM im Backend verwenden. Die *Passwortrichtlinie* gilt, wenn ein **Administrator** das Passwort eines Benutzers über UMC oder UDM ändert. Dies gilt auch, wenn ein **Benutzer** sein Passwort ändert und die UCS-Domäne **kein** Samba installiert hat.

[24] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

UCS definiert eine Standard-Passwortrichtlinie. *Passwortrichtlinieneinstellungen in UMC* (Seite 122) beschreibt die verfügbaren Einstellungen für die *Passwortrichtlinie*.

Sie können die *Passwort-Qualitätsprüfung* mit Univention Configuration Registry Variablen erweitern, wie in *Passwortrichtlinieneinstellungen in UMC* (Seite 122) erwähnt.

Sie können zusätzliche Passwortrichtlinien erstellen und sie den Benutzerkonten im LDAP-Verzeichnisbaum zuweisen. Weitere Informationen über Richtlinien finden Sie unter *Richtlinien* (Seite 77).

Wichtig: Wenn Sie Samba installiert haben, entwerfen Sie die Einstellungen für die Passwortanforderungen der Benutzerpasswortrichtlinie so, dass sie mit dem Samba-Domänenobjekt identisch ist, wie in *Passwort-Einstellungen für Windows-Clients bei Verwendung von Samba* (Seite 123) beschrieben.

Passwortrichtlinie für die Samba-Domäne
Wenn Sie Samba in Ihrer UCS-Domäne installiert haben, hat die Samba-Domäne eine eigene Passwortrichtlinie. UCS wendet die Samba-Passwortrichtlinie an, wenn ein **Benutzer** sein Passwort ändert, egal über welchen Dienst, über das Univention Portal, den User Self Service, Microsoft Windows oder Kerberos.

Um die Passwortrichtlinie für die Samba-Domäne zu konfigurieren, siehe *Passwort-Einstellungen für Windows-Clients bei Verwendung von Samba* (Seite 123).

Siehe auch:

***Installation* (Seite 177) von Samba**
für weitere Informationen über die Installation von Samba.

***Services für Windows* (Seite 177)**
für allgemeine Informationen über die Services für Windows.

6.3.2 Ändern des Benutzerpassworts

Das Ändern des Benutzerpassworts hat folgende Auslöser:

1. Das System fordert den Benutzer auf, sein Passwort zu ändern, z. B. weil das Passwort sein Ablaufdatum erreicht hat.
2. Durch eine Einstellung am Benutzerkonto, fordert ein Administrator den Benutzer auf, sein Passwort bei der nächsten Anmeldung zu ändern.
3. Der Benutzer beschließt, sein Passwort zu ändern.

Wenn ein Benutzer sein Passwort ändern möchte, kann er dies auf folgende Weise tun:

Univention Portal
In jeder UCS-Domäne ist das *Portal* installiert. Um das Passwort zu ändern, gehen Sie wie folgt vor:

1. Melden Sie sich am *Univention Portal* an.
2. Navigieren Sie zum Benutzermenü. Es ist das *„Burger-Menü“* in der oberen rechten Ecke.
3. Wählen Sie *Benutzereinstellungen ▸ Ihr Passwort ändern* aus.
4. Geben Sie Ihr aktuelles Passwort ein und setzen Sie ein neues Passwort. Geben Sie es erneut ein und bestätigen Sie es.

Benutzer Selbstverwaltung
Die *Benutzer Selbstverwaltung* (Seite 124) ist eine eigene App im *Univention App Center* (Seite 96). Sie bietet einen direkten Link zur Passwortänderung, so dass Administratoren eine prominente Kachel im Univention Portal für die Passwortänderung hinzufügen können. Außerdem bietet die App eine Möglichkeit, das Passwort der Benutzer zurückzusetzen, wenn diese es vergessen haben.

Microsoft Windows
Benutzer können ihr Benutzerpasswort über ihren Microsoft Windows-Client ändern, der über Samba mit der UCS-Domäne verbunden ist.

Kerberos
: Benutzer können ihr Benutzerpasswort über Clients ändern, die der UCS-Domäne über Kerberos beigetreten sind. Sie können die Standardfunktionen zur Änderung des Passworts dieser Clients verwenden.

  Für weitere Informationen über die Einbindung von Ubuntu- und Linux-Systemen in eine UCS Domäne und die Integration mit Kerberos, siehe *Extended domain services documentation* [2].

6.3.3 Passwortrichtlinieneinstellungen in UMC

Mit den Einstellungen der Passwortrichtlinie in UMC können Administratoren die Mindestpasswortlänge, das Ablaufintervall und die Länge der Passworthistorie festlegen. Abb. 6.7 zeigt die Einstellungen der Passwortrichtlinie in UMC. Im Anschluss an die Abbildung finden Sie einen Referenz der verfügbaren Einstellungen.

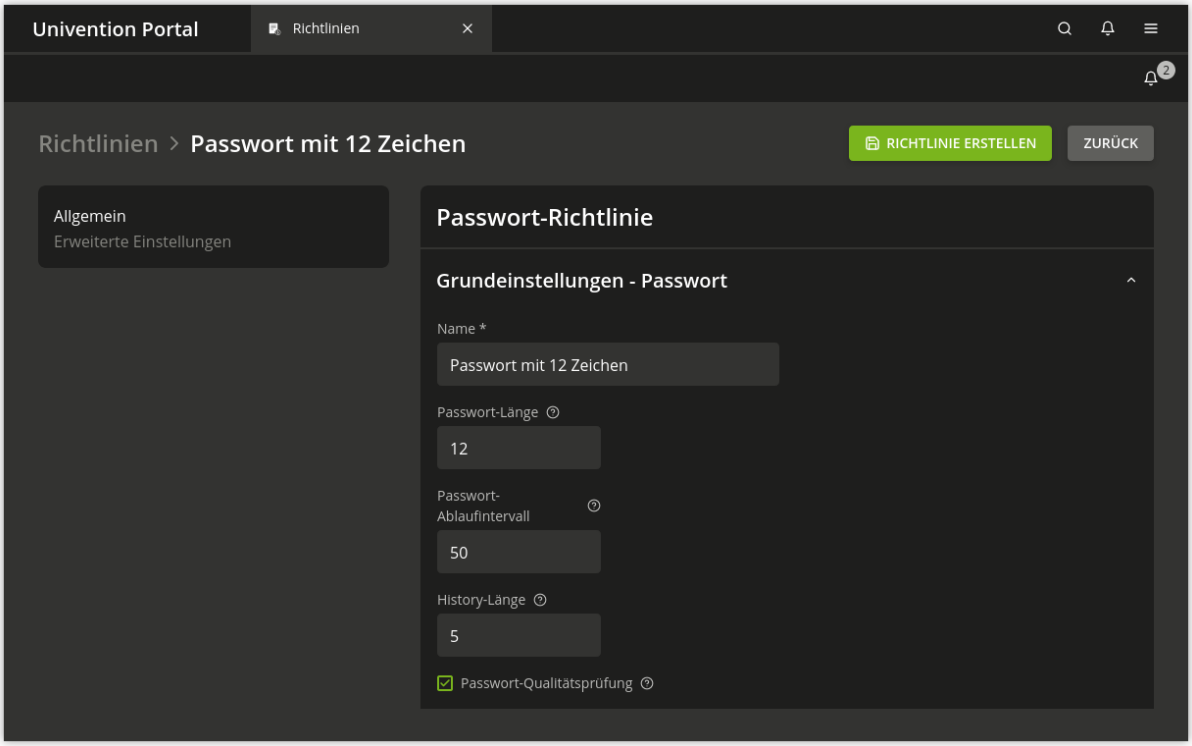


Abb. 6.7: Konfiguration einer Passwortrichtlinie

Auf dem Reiter *Allgemein* einer Passwortwortrichtlinie können Sie die folgenden Einstellungen vornehmen.

Passworthistorie
: Der Passworthistorie speichert die zuletzt verwendeten Passwort-Hashes. Die *History Länge* bestimmt die Länge der Historie, zum Beispiel, ob die Historie die letzten drei oder die letzten sieben Passwort-Hashes speichert. Benutzer können keine Passwörter aus der Passworthistorie wiederverwenden, um ein neues Passwort festzulegen. UCS speichert die Passwörter nicht rückwirkend.

  Um die Überprüfung der Passworthistorie zu deaktivieren, setzen Sie den Wert auf `0`.

  Beispiel
  : Wenn UCS zehn Passwort-Hashes gespeichert hat und Sie den Wert für die Länge der Passworthistorie auf `3` reduzieren, löscht UCS bei der nächsten Passwortänderung die älteren sieben Passwörter aus der Passworthistorie. Wenn Sie dann die Länge der Passworthistorie vergrößern, bleibt die Anzahl der gespeicherten Passwörter bei drei und erhöht sich mit jeder Passwortänderung.

Passwortlänge
: Die *Passwortlänge* ist die Mindestlänge in Zeichen, die ein Benutzerpasswort einhalten muss. Wenn Sie keinen Wert angeben, verwendet UCS die Mindestlänge von `8` Zeichen.

Der Standardwert gilt immer, wenn Sie keine Richtlinie festlegen und Sie das Kontrollkästchen *Passwortprüfung außer Kraft setzen* aktiviert haben. Das heißt, er gilt auch wenn Sie die Passwortrichtlinie *Standard-Einstellungen* gelöscht haben.

Um die Überprüfung der Passwortlänge zu deaktivieren, setzen Sie den Wert auf `0`.

Sie können einen Standardwert pro UCS-System über die Univention Configuration Registry Variable `password/quality/length/min` (Seite 315) konfigurieren. Die Einstellung gilt für Benutzer, die nicht einer *UDM-Passwortrichtlinie* unterliegen.

Passwortablaufintervall
Ein *Passwort-Ablaufintervall* verlangt regelmäßige Passwortänderungen. UCS verlangt von einem Benutzer, dass er sein Passwort bei der Anmeldung an der UCS Web-Oberfläche, an Kerberos, und an UCS-Systemen ändert, wenn das Ablaufintervall verstrichen ist. UCS zeigt die Restlaufzeit des Benutzerpasswortes im Benutzerverwaltungsmodul unter *Passwortablaufdatum* im Reiter *Konto* an.

Um das *Passwort-Ablaufintervall* zu deaktivieren, lassen Sie den Wert leer.

Passwortqualitätsprüfung
Wenn Sie die Option *Passwortqualitätsprüfung* aktivieren, führt UCS zusätzliche Passwortprüfungen, einschließlich Wörterbuchprüfungen, für Passwortänderungen in UMC und Kerberos durch.

Sie konfigurieren die Qualitätsprüfungen über die folgenden Univention Configuration Registry Variablen. Weitere Informationen finden Sie in den verlinkten Variablenbeschreibungen.

Sie können die folgenden Kontrollen erzwingen:

- `password/quality/credit/digits` (Seite 315)
- `password/quality/credit/upper` (Seite 315)
- `password/quality/credit/lower` (Seite 315)
- `password/quality/credit/other` (Seite 315)
- `password/quality/forbidden/chars` (Seite 315)
- `password/quality/required/chars` (Seite 315)
- `password/quality/mspolicy` (Seite 315)

Wichtig: Um die *Passwortqualitätsprüfung* auf alle UCS Anmeldesysteme anzuwenden, müssen Sie die Univention Configuration Registry Variablen auf **allen** UCS Anmeldeservern setzen.

6.4 Passwort-Einstellungen für Windows-Clients bei Verwendung von Samba

Mit dem Samba-Domänenobjekt können Sie die Anforderungen an Passwörter für Benutzerkonten in einer Samba-Domäne festlegen.

Sie können das Samba-Domänenobjekt über das UMC-Modul *LDAP-Verzeichnis* verwalten. Das Samba-Domänen-Objekt befindet sich im `samba`-Container und hat den NetBIOS-Namen der Domäne. Sie finden den `samba`-Container unter der LDAP-Basis.

Wichtig: Es wird dringend empfohlen, die Einstellungen der Passwortanforderungen des Samba-Domänenobjekts identisch mit der Benutzerpasswortrichtlinie zu gestalten, wie in *Verwaltung der Benutzerpasswörter* (Seite 120) beschrieben.

Im Abschnitt *Passwort* auf dem Reiter *Allgemein* des Objekts *Samba Domain* können Sie die folgenden Einstellungen vornehmen.

Passwortlänge
Die Anzahl an Zeichen, die ein Benutzerpasswort mindestens enthalten muss.

Passworthistorie
UCS speichert Passwortänderungen in Form von Hashes. Benutzer können keine Passwörter aus der Historie verwenden, wenn sie ein Passwort setzen. Zum Beispiel, mit einem Wert für die Länge der Passworthistorie von `5` muss der Benutzer fünf andere Passwörter festlegen, bevor er ein Passwort aus der Historie wiederverwenden kann.

Minimales Passwortalter
Legt die Zeitspanne fest, die vergehen muss, bevor die Benutzer ihr ihr Passwort ändern können.

Maximales Passwortalter
Legt das maximale Alter für ein Passwort fest. Nach Ablauf dieser Zeitspanne, fordert UCS den Benutzer auf, sein Passwort bei der nächsten Anmeldung zu ändern.

Um eine unendliche Zeitspanne zu definieren, lassen Sie den Wert leer.

Das Passwort muss die Komplexitätsanforderungen erfüllen
Das Aktivieren des Kontrollkästchens aktiviert die Microsoft Password complexity Anforderungen[25]. Ein Tooltip zeigt die erforderlichen Zeichen in einem Passwort an. Die Bibliothek `Passfilt.dll` erzwingt die Komplexitätsanforderungen. Administratoren können sie nicht ändern.

6.5 Benutzer Selbstverwaltung

Informationen zum Festlegen einer Benutzer-Passwortrichtlinie finden Sie unter *Verwaltung der Benutzerpasswörter* (Seite 120).

6.5.1 Passwortwechsel über UCS Portal

Jeder angemeldete Benutzer kann sein eigenes Passwort ändern, indem er das Menü in der oberen rechten Ecke öffnet und *Benutzereinstellungen* ▸ *Passwort ändern* auswählt. Die Änderung wird dann direkt über den PAM-Stack (siehe *Authentifizierung / PAM* (Seite 167)) durchgeführt und ist danach zentral für alle Dienste verfügbar.

6.5.2 Passwort-Verwaltung über Self Service App

Durch die Installation der UCS-Komponenten **`Self Service Backend`** auf dem UCS Primary Directory Node und **`Self Service`** in der Domäne über das *App Center* werden Benutzer dazu befähigt, ihr Passwort ohne die Interaktion mit einem Administrator zu verwalten.

Die *Self Service* App erzeugt ein eigenes Portal, das unter `/univention/selfservice/` aufgerufen werden kann und alle Funktionen über entsprechende Einträge zur Verfügung stellt. Es werden aber auch im eigentlichen Portal verschiedene Menüeinträge im Benutzermenü registriert. Sie erlauben es Benutzern, unter Angabe ihres alten Passworts ein neues Passwort zu setzen, oder aber ihr vergessenes Passwort zurückzusetzen. Für das Zurücksetzen des Passworts wird ein Token an eine vorher dafür registrierte Kontakt-E-Mail-Adresse gesendet, das dann auf der Webseite vom Benutzer einzugeben ist.

Mit den folgenden Univention Configuration Registry Variablen können einzelne Funktionen der Passwort-Verwaltung aktiviert oder deaktiviert werden.

`umc/self-service/passwordreset/backend/enabled`
Aktiviert oder deaktiviert die Backend-Funktionalität der *Passwort vergessen*-Seite. Diese Univention Configuration Registry muss auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry Variable *`self-service/backend-server`* (Seite 317) definiert ist, da Anfragen bezüglich dieser Variablen an das *Self Service Backend* weitergeleitet werden.

[25] https://learn.microsoft.com/de-de/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

umc/self-service/protect-account/backend/enabled

Aktiviert oder deaktiviert die Backend-Funktionalität der *Kontozugang schützen*-Seite. Diese Univention Configuration Registry muss auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry Variable `self-service/backend-server` (Seite 317) definiert ist, da Anfragen bezüglich dieser Variablen an das *Self Service Backend* weitergeleitet werden.

umc/self-service/service-specific-passwords/backend/enabled

Aktiviert oder deaktiviert die Backend-Funktionalität für dienst-spezifische Passwörter. Momentan wird nur RADIUS als Dienst unterstützt. Weitere Informationen finden sich in *Dienst-spezifisches Passwort* (Seite 240).

Die entsprechenden Einträge im Portal werden damit auch aktiviert oder deaktiviert. Sie können die Einträge aber auch manuell anpassen. Sie verhalten sich wie normale Einträge im Portal.

6.5.3 Profilverwaltung

Am Benutzerkonto im LDAP-Verzeichnisdienst können weitere personenbezogene Daten gespeichert werden. Dies beinhaltet u.a. ein Bild, private Adressen und weitere Kontaktinformationen. Standardmäßig können diese nur von Administratoren aktualisiert werden. Alternativ können aber auch ausgewählte Felder für den Benutzer selber freigeschaltet werden. Der kann diese Daten über die *Self Service* App selber pflegen.

Dafür müssen folgende Univention Configuration Registry Variablen konfiguriert werden:

self-service/ldap_attributes

Über diese Variable werden die *LDAP* Attribute konfiguriert, die ein Benutzer selber an seinem Benutzerkonto modifizieren kann. Die Namen der Attribute sind durch Komma zu trennen. Diese Variable ist auf dem Primary Directory Node (und Backup Directory Nodes) zu setzen.

self-service/udm_attributes

Über diese Variable werden die *UDM* Attribute konfiguriert, die ein Benutzer modifizieren kann. Die Namen der Attribute sind durch Komma zu trennen. Diese Variable ist auf allen beteiligten Server-Systemen zu setzen, auf denen die *Self Service* App installiert ist (ebenso auf dem Primary Directory Node).

self-service/udm_attributes/read-only

Diese Variable setzt *UDM* Attribute, welche in Univention Configuration Registry Variable `self-service/udm_attributes` (Seite 125) gesetzt sind, auf schreibgeschützt. Trennen Sie mehrere Werte durch Kommata. Setzen Sie diese Variable auf allen Hosts, auf denen die **Self Service** App installiert ist, einschließlich Primary Directory Node.

Entfernen Sie die *LDAP* Attribute, welche in Univention Configuration Registry Variable `self-service/ldap_attributes` (Seite 125) gesetzt sind und schreibgeschützt werden sollen, damit diese Variable wie vorgesehen funktioniert. Andernfalls werden diese *LDAP* Attribute verhindern, dass die in dieser Variable angegebenen *UDM* Attribute schreibgeschützt werden.

umc/self-service/profiledata/enabled

Diese Variable muss auf allen beteiligten Server-Systemen auf `true` gesetzt werden, um den Mechanismus zu aktivieren.

umc/self-service/allow-authenticated-use

Diese Variable definiert, ob beim Öffnen und Modifizieren des eigenen Benutzerprofils die Angabe von Benutzername und Passwort notwendig ist, wenn man bereits am Univention Portal angemeldet ist.

Ab UCS 4.4-7 wird diese Univention Configuration Registry Variable bei Erstinstallationen des *Self Service* automatisch auf `true` gesetzt, was die Verwendung einer vorhandenen Portalsitzung aktiviert. Die Felder *Benutzername* und *Passwort* werden dann automatisch ausgefüllt oder nicht mehr angezeigt.

Systeme, die auf UCS 4.4-7 aktualisiert werden, behalten die alte Verhaltensweise bei, indem automatisch der Wert auf `false` gesetzt wird. Es ist zu beachten, dass diese Variable auf allen beteiligen Systemen inklusive Primary Directory Node auf den gleichen Wert gesetzt sein muss.

Beide `*attributes` Variablen müssen zueinander passen. Die Namen der Attribute und deren Zuordnung kann man über folgenden Aufruf erhalten:

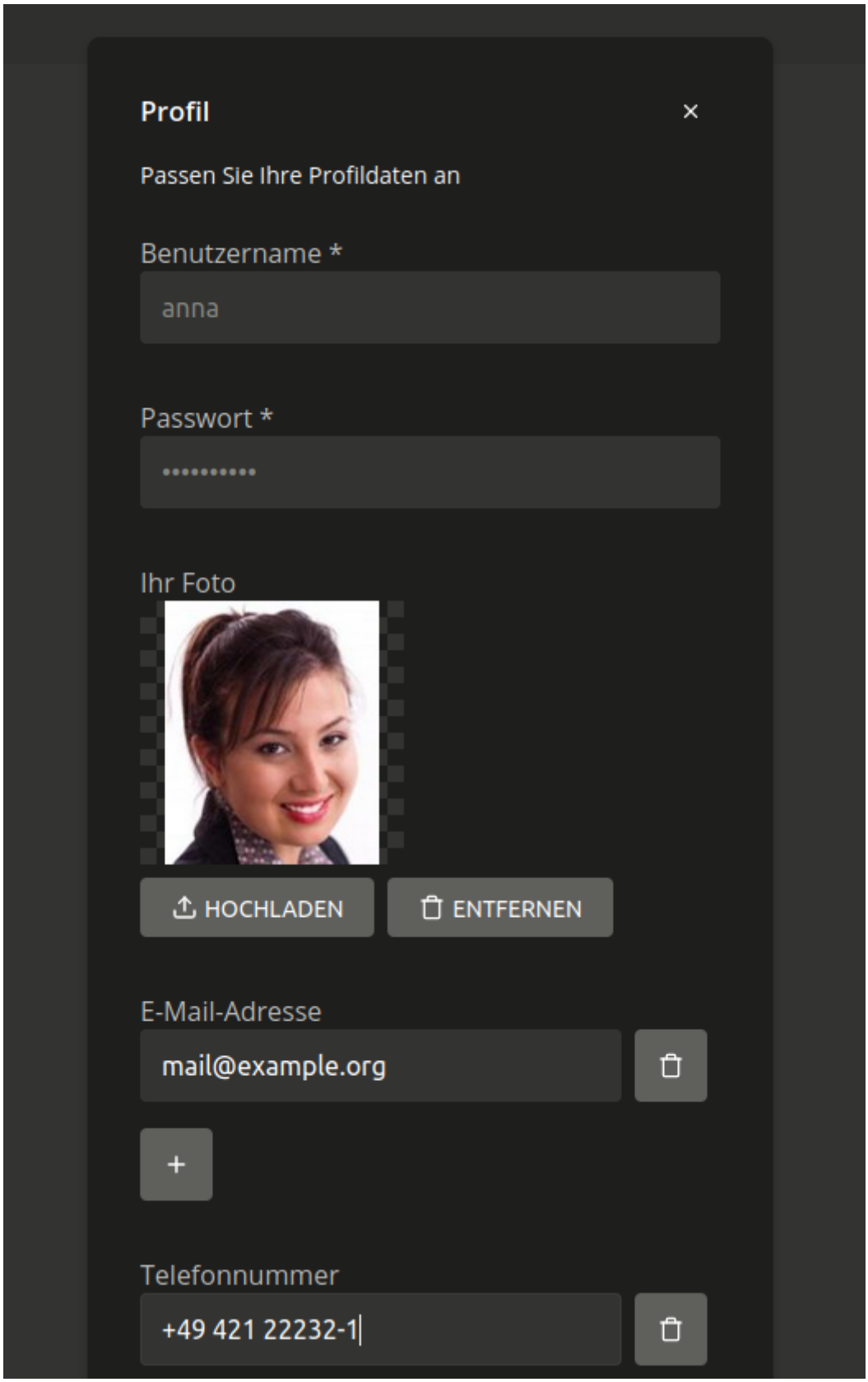


Abb. 6.8: Benutzerprofilselbstverwaltung

```
$ python3 -c 'from univention.admin.handlers.users.user import mapping;\
  print("\n".join( \
  map("{0[0]:>30s} {0[1][0]:<30s}".format, sorted(mapping._map.items()))) \
  )'
```

6.5.4 Selbstregistrierung

Der *Self Service* ermöglicht es Benutzern, sich selbst zu registrieren, wodurch ein Benutzerkonto erstellt wird, das per E-Mail verifiziert werden muss.

Bei Benutzerkonten, die über den *Self Service* erstellt werden, wird das `RegisteredThroughSelfService` Attribut des Benutzers auf `TRUE` und das `PasswordRecoveryEmailVerified` Attribut auf `FALSE` gesetzt. Nachdem der Benutzer sein Konto über die Verifizierungsmail verifiziert hat, wird das `PasswordRecoveryEmailVerified` Attribut auf `TRUE` gesetzt.

Kontoerstellung

Aspekte der *Konto erstellen* Seite und der Kontoerstellung selbst können mit den folgenden Univention Configuration Registry Variablen konfiguriert werden. Diese Variablen müssen auf dem **`Self Service Backend`** gesetzt werden, das über die Univention Configuration Registry Variable *`self-service/backend-server`* (Seite 317) definiert ist, da Anfragen bezüglich dieser Variablen an das Self Service Backend weitergeleitet werden.

`umc/self-service/account-registration/backend/enabled`
: Mit dieser Variable kann die Selbstregistrierung deaktiviert/aktiviert werden.

`umc/self-service/account-registration/usertemplate`
: Mit dieser Variable kann eine *Benutzervorlage* (Seite 134) angegeben werden, die für die Erstellung von selbst registrierten Konten verwendet wird.

`umc/self-service/account-registration/usercontainer`
: Mit dieser Variable kann ein Container angegeben werden, unter dem die selbst registrierten Benutzer angelegt werden.

`umc/self-service/account-registration/udm_attributes`
: Diese Variable konfiguriert, welche UDM-Attribute eines Benutzerkontos auf der Seite *Konto erstellen* des *Self Service* angezeigt werden. Die Namen der UDM-Attribute müssen als kommaseparierte Liste angegeben werden.

`umc/self-service/account-registration/udm_attributes/required`
: Diese Variable konfiguriert, welche der über die Univention Configuration Registry Variable *`umc/self-service/account-registration/udm_attributes`* (Seite 127) definierten UDM-Attribute vom Benutzer angegeben werden müssen. Die Namen der UDM-Attribute müssen als kommaseparierte Liste angegeben werden.

Verifizierungsmail

Nachdem ein Benutzer auf *Konto erstellen* geklickt hat, sieht er eine Nachricht, dass eine E-Mail für die Kontoverifizierung versendet wurde.

Aspekte der *Verifizierungsmail* und des Verifizierungstokens können über die folgenden Univention Configuration Registry Variablen konfiguriert werden. Diese Variablen müssen auf dem *Self Service Backend* gesetzt werden, der über die Univention Configuration Registry Variable *`self-service/backend-server`* (Seite 317) definiert ist, da Anfragen bezüglich dieser Variablen an den *Self Service Backend* weitergeleitet werden.

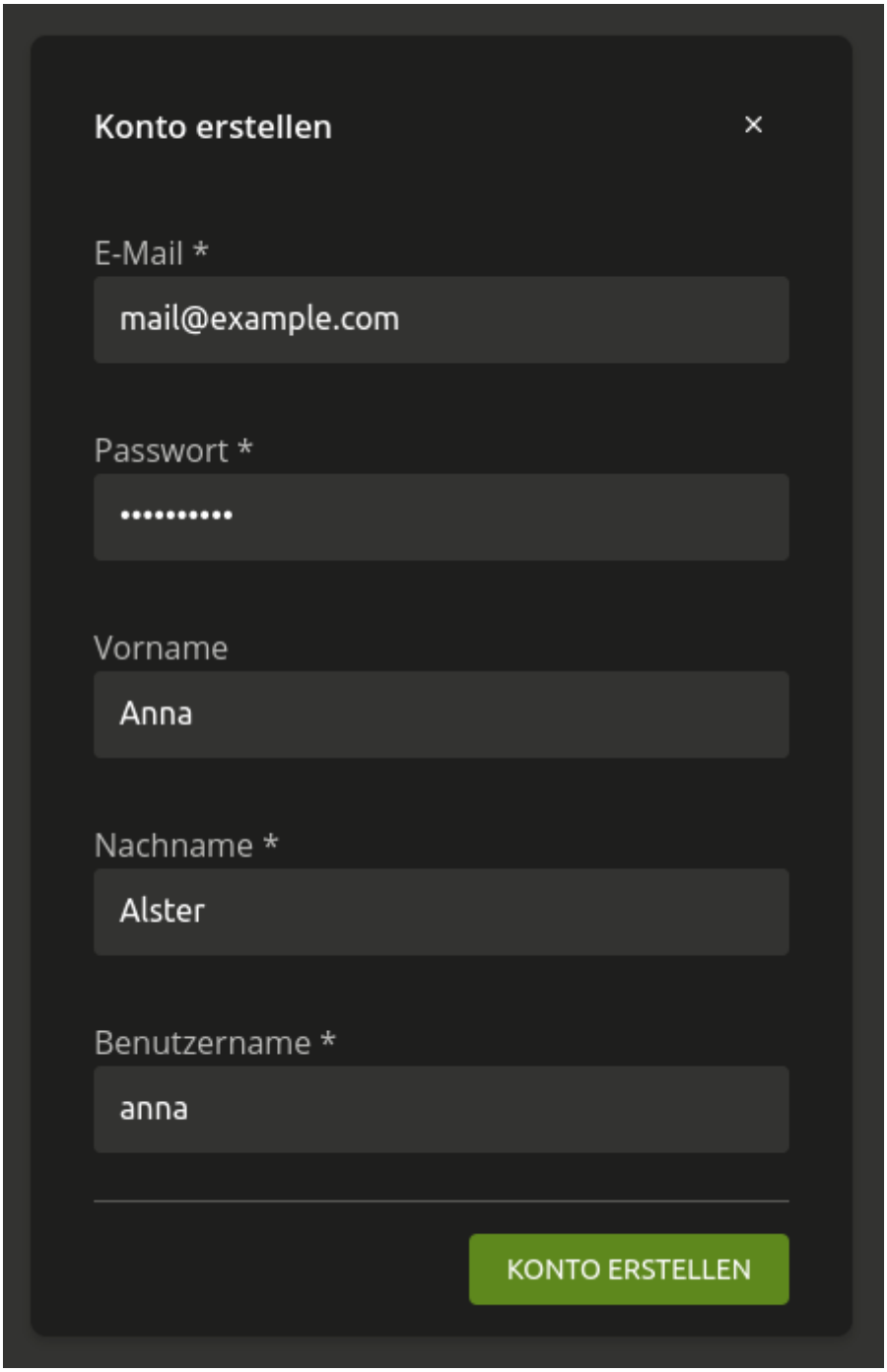


Abb. 6.9: Selbstregistrierung

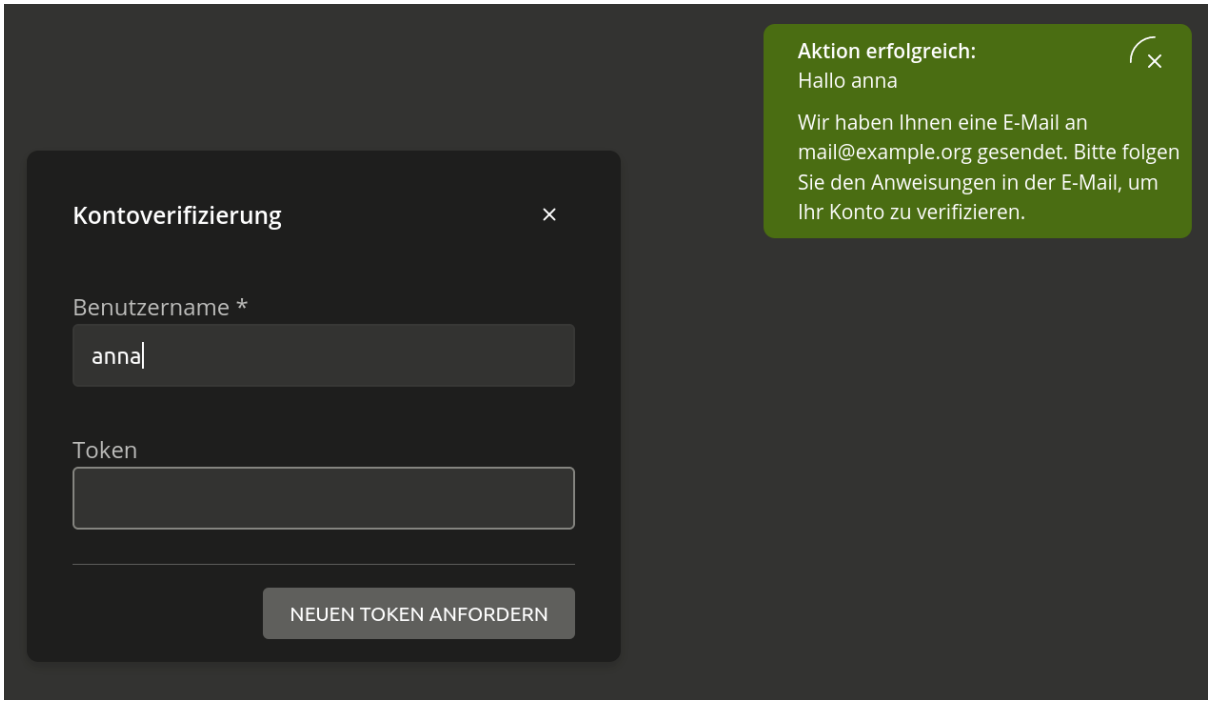


Abb. 6.10: Senden der Verifizierungsmail

umc/self-service/account-verification/email/webserver_address

Definiert den `host` Teil, der in dem Verifizierungslink verwendet werden soll. Standardmäßig wird der FQDN des über die Univention Configuration Registry Variable *self-service/backend-server* (Seite 317) definierten **Self Service Backend** verwendet, da diese Univention Configuration Registry Variable dort ausgewertet wird.

umc/self-service/account-verification/email/sender_address

Definiert die Absenderadresse der Verifizierungsmail. Die Voreinstellung ist `Account Verification Service <noreply@`*FQDN*`>`.

umc/self-service/account-verification/email/server

Servername oder IP-Adresse des zu verwendenden Mail-Servers.

umc/self-service/account-verification/email/text_file

Ein Pfad zu einer Textdatei, deren Inhalt für den Körper der Verifizierungsmail verwendet wird. Der Text kann die folgenden Zeichenfolgen enthalten, die entsprechend ersetzt werden: `{link}`, `{token}`, `{tokenlink}` und `{username}`. Als Standard wird die Datei `/usr/share/univention-self-service/email_bodies/verification_email_body.txt` verwendet.

umc/self-service/account-verification/email/token_length

Definiert die Anzahl der Zeichen, die für den Verifizierungstoken verwendet wird. Als Standard werden 64 Zeichen verwendet.

Kontoverifizierung

Wenn der Benutzer dem Verifizierungslink aus der E-Mail folgt, gelangt er auf die Seite *Kontoverifizierung* des **Self Service**.

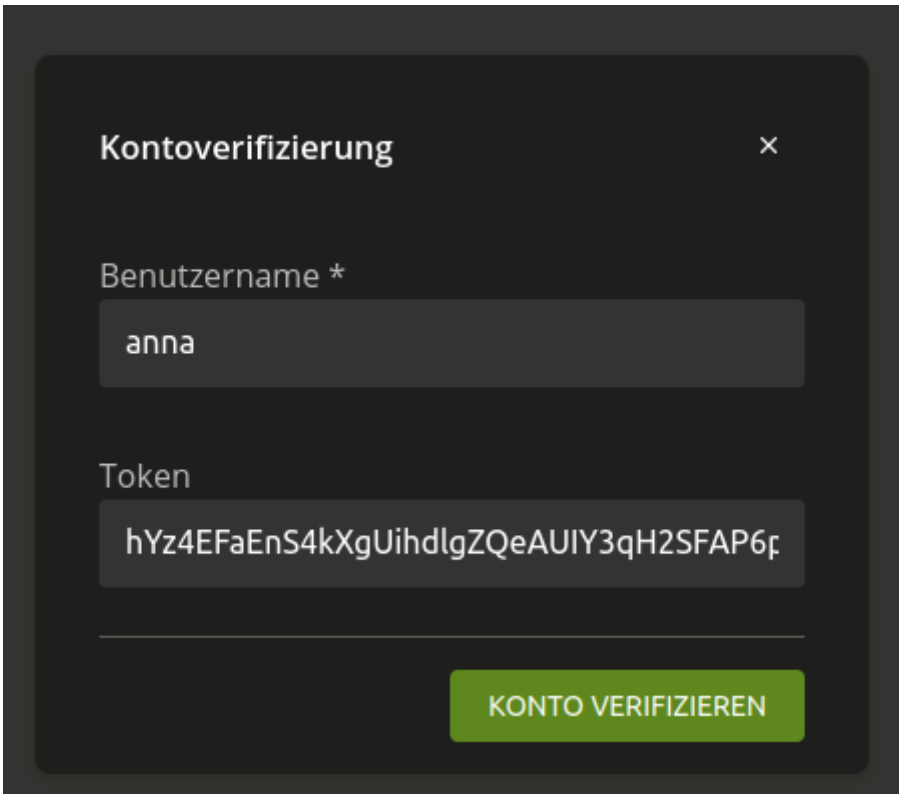


Abb. 6.11: Kontoverifizierung

Die Kontoverifizierung und die Anforderung neuer Verifizierungstoken kann mit der Univention Configuration Registry Variable *umc/self-service/account-verification/backend/enabled* (Seite 319) deaktiviert/aktiviert werden. Diese Variablen muss auf dem **Self Service Backend** gesetzt werden, das über die Univention Configuration Registry Variable *self-service/backend-server* (Seite 317) definiert ist.

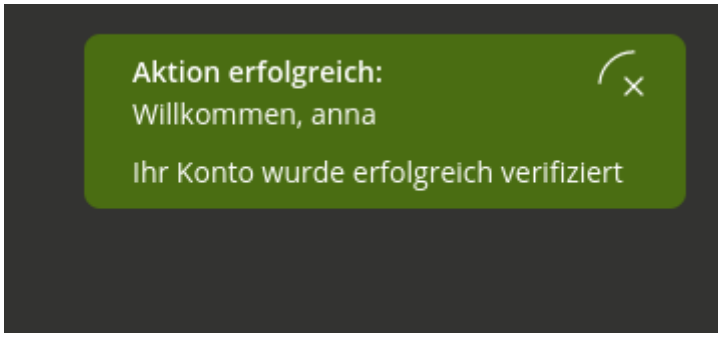


Abb. 6.12: Kontoverifizierung

Der SSO Login kann konfiguriert werden, die Anmeldung für unverifizierte, selbst registrierte Konten zu verbieten. Dies wird über die Univention Configuration Registry Variable *saml/idp/selfservice/check_email_verification* (Seite 317) konfiguriert. Diese Einstellung muss auf dem Primary Directory Node und allen Backup Directory Nodes vorgenommen werden. Für Konten, die durch einen Administrator angelegt wurden, hat diese Einstellung keine Auswirkung.

Die Nachricht, welche auf der SSO Login Seite für unverifizierte, selbst registrierte Konten angezeigt wird, kann mit den Univention Configuration Registry Variablen *saml/idp/selfservice/account-verification/*

error-title (Seite 317) und *saml/idp/selfservice/account-verification/error-descr* (Seite 317) konfiguriert werden. Eine lokalisierte Nachricht kann konfiguriert werden, indem eine *Locale* wie z.B. `de` an die Variable angehängt wird. Z.B. `saml/idp/selfservice/account-verification/error-title/`*de*.

Falls die **Keycloak** App als Identity Provider eingesetzt wird,schauen Sie bitte in der *Univention Keycloak app documentation* [4] unter Settings[26] für die entsprechenden Einstellungen.

6.5.5 Selbst-Deregistrierung

Der **Self Service** ermöglicht es Benutzern, die Löschung ihres eigenen Kontos zu beantragen. Diese Funktion kann mit der Univention Configuration Registry Variable *umc/self-service/account-deregistration/enabled* (Seite 319) aktiviert werden, wodurch der Button *Meinen Account löschen* auf der Seite *Ihr Profil* des *Self Service* angezeigt wird (*Benutzervorlagen* (Seite 134)).

Wenn ein Benutzer beantragt hat, sein Konto zu löschen, wird es nicht direkt gelöscht sondern deaktiviert. Zusätzlich wird das `DeregistredThroughSelfService` Attribut des Benutzers auf `TRUE` gesetzt und das `DeregistrationTimestamp` Attribut des Benutzers wird in der GeneralizedTime-LDAP-Syntax[27] auf die aktuelle Zeit gesetzt. Wenn der Benutzer eine `PasswordRecoveryEmail` angegeben hat, wird er eine E-Mail-Benachrichtigung erhalten, die mit den folgenden Univention Configuration Registry Variablen konfiguriert werden kann.

umc/self-service/account-deregistration/email/sender_address

Definiert die E-Mail-Adresse des Absenders für Benachrichtigung. Die Voreinstellung ist `Password Reset Service <noreply@`*FQDN*`>`.

umc/self-service/account-deregistration/email/server

Servername oder IP-Adresse des zu verwendenden Mail-Servers.

umc/self-service/account-deregistration/email/text_file

Ein Pfad zu einer Textdatei, deren Inhalt für den Körper der E-Mail verwendet wird. Der Text kann die folgenden Zeichenfolgen enthalten, die entsprechend ersetzt werden: `{username}`. Als Standard wird die Datei `/usr/share/univention-self-service/email_bodies/deregistration_notification_email_body.txt` verwendet.

Der *Self Service* stellt unter `/usr/share/univention-self-service/delete_deregistered_accounts.py` ein Skript zur Verfügung, das zum Löschen aller users/user Objekte verwendet werden kann, bei denen `DeregistredThroughSelfService` auf `TRUE` gesetzt ist und deren `DeregistrationTimestamp` älter ist als eine angegebene Zeit.

Der folgende Befehl würde Benutzer löschen, deren `DeregistrationTimestamp` älter als 5 Tage und 2 Stunden ist:

```
$ /usr/share/univention-self-service/delete_deregistered_accounts.py \
  --timedelta-days 5 \
  --timedelta-hours 2
```

Für alle möglichen Argumente zum Skript siehe:

```
$ /usr/share/univention-self-service/delete_deregistered_accounts.py --help
```

Das Skript kann regelmäßig ausgeführt werden, indem ein Cron-Job über Univention Configuration Registry erstellt wird.

```
$ ucr set cron/delete_deregistered_accounts/command=\
/usr/share/univention-self-service/delete_deregistered_accounts.py\
' --timedelta-days 30'\
  cron/delete_deregistered_accounts/time='00 06 * * *'  # daily at 06:00
```

[26] https://docs.software-univention.de/keycloak-app/latest/configuration.html#app-settings
[27] https://ldapwiki.com/wiki/Wiki.jsp?page=GeneralizedTime

Weitere Informationen über die Einstellung von Cron-Jobs über UCR können in *Definition eigener Cron-Jobs in Univention Configuration Registry* (Seite 173) gefunden werden.

6.6 Automatisches Sperren von Benutzern nach fehlgeschlagenen Anmeldungen

Standardmäßig kann ein Benutzer sein Passwort beliebig oft falsch eingeben. Um Brute Force-Angriffe auf Passwörter zu erschweren, kann eine automatische Sperre von einem Benutzerkonto nach einer konfigurierbaren Anzahl von fehlerhaften Anmeldungen aktiviert werden.

UCS vereinheitlicht verschiedene Methoden zur Authentifizierung und Autorisierung von Benutzern. Abhängig von den installierten Softwarekomponenten kann es verschiedene Mechanismen geben, wie fehlgeschlagene Anmeldeversuche konfiguriert und gezählt werden.

Im folgenden werden die drei unterschiedlichen Methoden beschrieben.

6.6.1 Samba Active Directory Dienste

In Samba Active Directory Umgebungen werden diverse Dienste von Samba bereitgestellt, wie zum Beispiel Kerberos. Um Benutzer nach fehlgeschlagenen Anmeldungen zu sperren, kann das Tool **samba-tool** verwendet werden.

- Um die aktuell konfigurierten Werte anzuzeigen:

```
$ samba-tool domain passwordsettings show
```

- Um festzulegen, wie oft ein Benutzer versuchen kann, sich mit einem falschen Passwort anzumelden, bevor das Konto gesperrt wird:

```
$ samba-tool domain passwordsettings set --account-lockout-threshold=5
```

- Um festzulegen, wie viele Minuten ein Konto gesperrt wird, nachdem zu viele falsche Passwörter eingegeben wurden:

```
$ samba-tool domain passwordsettings set --account-lockout-duration=3
```

- Um die Anzahl der Minuten festzulegen, nach der der Zähler zurückgesetzt wird:

```
$ samba-tool domain passwordsettings set --reset-account-lockout-after=5
```

  Wenn ein Konto automatisch nach der konfigurierten Aussperrungsdauer entsperrt wird, dann wird der Zähler nicht direkt mit zurückgesetzt, um das Konto noch eine gewisse Zeit unter strikter Beobachtung zu halten. In dem Zeitfenster nach dem Ende der Aussperrung und vor der endgültigen Rücksetzung des Zählers führt ein einziger erneuter Login-Versuch mit einem falschen Passwort direkt wieder zu einer Sperrung des Kontos.

Die manuelle Entsperrung eines Benutzers erfolgt in der Benutzerverwaltung auf dem Reiter *Konto* über die Aktivierung der Checkbox *Aussperrung zurücksetzen*.

6.6.2 PAM-Stack

Das automatische Sperren von Benutzern nach fehlgeschlagenen Anmeldungen im PAM-Stack kann durch Setzen der Univention Configuration Registry Variable *auth/faillog* (Seite 303) auf `yes` aktiviert werden. Die Obergrenze an fehlerhaften Passworteingaben, bei der eine Kontosperre aktiviert wird, wird in der Univention Configuration Registry Variable *auth/faillog/limit* (Seite 303) konfiguriert. Unterhalb des Limits wird nach einer korrekten Passworteingabe der Zähler jedesmal wieder zurückgesetzt.

Die Sperre im PAM-Stack ist standardmäßig nur auf ein lokales System begrenzt. Wenn ein Benutzer also auf einem System zu oft sein Passwort falsch eingegeben hat, kann er sich auf einem anderen System weiterhin anmelden. Durch Setzen der Univention Configuration Registry Variable *auth/faillog/lock_global* (Seite 303) kann die Sperre auch global erfolgen und wird im LDAP registriert. Die globale Sperrung kann nur auf Primary Directory Node/Backup-Systemen eingesetzt werden, da andere Systemrollen nicht über die nötigen Berechtigungen im LDAP-Verzeichnis verfügen. Auf allen Servern der genannten Systemrollen wird die Aussperrung aber automatisch auch lokal umgesetzt oder über das verwendete Listener-Modul auch wieder zurückgenommen, abhängig vom aktuellen Aussperrungszustands des Kontos im LDAP-Verzeichnis.

Standardmäßig ist die Sperre über den PAM-Stack unbegrenzt gültig, sie kann aber auch nach Ablauf eines Intervalls automatisch wieder aufgehoben werden. Hierzu ist in der Univention Configuration Registry Variable *auth/faillog/unlock_time* (Seite 303) ein Zeitraum in Sekunden anzugeben. Wird der Wert auf `0` gesetzt, wird die Sperre direkt wiederaufgehoben.

Der `root`-Benutzer ist standardmäßig von der Passwort-Sperre ausgenommen, kann aber durch Setzen der Univention Configuration Registry Variable *auth/faillog/root* (Seite 303) auf `yes` ebenfalls aufgenommen werden.

Werden Konten nur lokal gesperrt, kann der Administrator ein Benutzerkonto durch Eingabe des folgenden Befehls entsperren:

```
$ faillog -r -u USERNAME
```

Erfolgt die Sperrung global im LDAP, kann der Benutzer im UMC-Modul *Benutzer* unter dem Reiter *Konto* mit der Optionen *Aussperrung zurücksetzen* zurückgesetzt werden.

6.6.3 OpenLDAP

Bei UCS Directory Nodes kann die automatische Kontosperre für den Fall eines wiederholten LDAP-Authentifizierungsfehlers aktiviert werden. Voraussetzung ist, dass das MDB LDAP-Backend verwendet wird. Dies ist seit UCS 4 das Standard Backend, vorherige Systeme müssen auf das MDB LDAP-Backend migriert werden, siehe *UCS performance guide* [5].

Die Aktivierung der automatischen Kontosperrung muss pro UCS Directory Node aktiviert werden. Dazu müssen die Univention Configuration Registry Variablen *ldap/ppolicy* (Seite 309) und *ldap/ppolicy/enabled* (Seite 309) auf `yes` gesetzt werden und der OpenLDAP Server muss neu gestartet werden:

```
$ ucr set ldap/ppolicy=yes ldap/ppolicy/enabled=yes
$ systemctl restart slapd
```

Die Standardrichtlinie ist so ausgelegt, dass fünf wiederholte LDAP-Authentifizierungsfehler innerhalb eines Überwachungsintervalls von fünf Minuten dazu führen, dass das authentifizierende Konto gesperrt wird. Ein gesperrtes Konto kann nur von einem Domain-Administrator über das UMC-Modul *Benutzer* über die Checkbox *Aussperrung zurücksetzen* im Reiter *Konto* freigeschaltet werden.

Die Anzahl der wiederholten LDAP-Authentifizierungsfehler kann in dem Konfigurationsobjekt mit der *objectClass* `pwdPolicy` angepasst werden:

```
$ univention-ldapsearch objectclass=pwdPolicy
```

pwdMaxFailure
: Das Attribut bestimmt die Anzahl der LDAP-Authentifizierungsfehler vor der Sperrung.

pwdMaxFailureCountInterval
: Das Attribut bestimmt das Zeitintervall in Sekunden, das berücksichtigt wird. LDAP-Authentifizierungsfehler außerhalb dieses Intervalls werden bei der Zählung vernachlässigt.

Um den Account erst nach 10 Versuchen zu sperren kann der folgende Befehl verwendet werden:

```
$ LB="$(ucr get ldap/base)"
$ ldapmodify -x -D "cn=admin,$LB" -y /etc/ldap.secret <<__EOT__
dn: cn=default,cn=ppolicy,cn=univention,$LB
changetype: modify
replace: pwdMaxFailure
pwdMaxFailure: 10
__EOT__
```

Die manuelle Entsperrung eines Benutzers erfolgt in der Benutzerverwaltung auf dem Reiter *Konto* über die Aktivierung der Checkbox *Aussperrung zurücksetzen*.

6.7 Benutzervorlagen

Mit einer Benutzervorlage können beim Anlegen eines Benutzers Einstellungen vorgegeben werden. Ist mindestens eine Benutzervorlage definiert, kann sie beim Anlegen eines Benutzer ausgewählt werden.

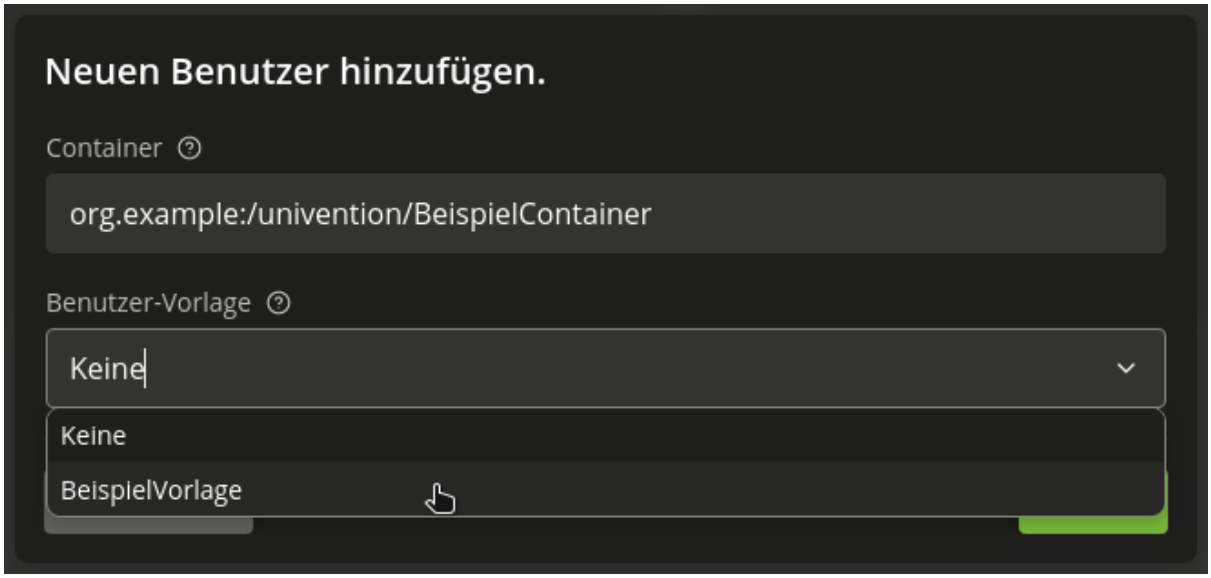


Abb. 6.13: Auswahl einer Benutzervorlage

Benutzervorlagen werden im UMC-Modul *LDAP-Verzeichnis* verwaltet. Dort muss in den Container `univention` und dort in den Untercontainer `templates` gewechselt werden. Hier kann über *Hinzufügen* mit dem Objekt-Typ `Einstellungen: Benutzervorlage` eine neue Benutzervorlage angelegt werden.

In einer Benutzervorlage kann entweder ein fester Wert vorgegeben werden (z.B. für die Anschrift) oder ein Attribut der Benutzerverwaltung referenziert werden. Attribute werden dabei in spitzen Klammern referenziert.

Eine Liste möglicher Attribute kann mit dem folgenden Befehl im Abschnitt *users/user variables* der Ausgabe angezeigt werden:

```
$ univention-director-manager users/user
```

Wird beim Hinzufügen eines Benutzers eine Benutzervorlage verwendet, überschreibt diese alle in der Vorlage vorkommenden Felder mit dem in der Vorlage gesetzten Wert. Dabei gilt ein leeres Feld ebenfalls als auf `""` gesetzt.

Es können auch nur Teilwerte von Attributen übernommen werden und Werte in Groß-/Kleinschreibung konvertiert werden.

So kann beispielsweise das UNIX-Heimatverzeichnis unter `/home/<title>.<lastname>` angelegt werden oder die primäre E-Mail-Adresse mit `<firstname>.<lastname>@firma.com` vordefiniert werden. Ersetzungen sind grundsätzlich für beliebige Werte möglich, eine syntaktische oder semantische Überprüfung erfolgt jedoch nicht. Wird beispielsweise beim Anlegen des Benutzers kein Vorname angegeben, würde die obige E-Mail-Adresse mit einem Punkt beginnen und wäre somit nach dem E-Mail-Standard ungültig. Ähnliche Fehlerquellen können auch im Umgang mit Dateipfaden auftreten. Nicht auflösbare Attribute (etwa durch Tippfehler in der Vorlage) werden gelöscht.

Wird nicht der komplette Attributwert, sondern nur ein einzelnes Zeichen des Attributs benötigt, kann in der Benutzervorlage nach dem Attributnamen der Index des benötigten Zeichens in eckigen Klammern angegeben werden. Die Zählung der Zeichen des Attributs beginnt bei `0`, so dass z.B. der Index `1` dem zweiten Zeichen des Attributwertes entspricht. Mit `<firstname>[0].<lastname>@firma.com` wird beispielsweise eine E-Mail-Adresse aus dem ersten Buchstaben des Vornamens sowie dem Nachnamen gebildet.

Eine Teilzeichenkette des Attributwerts kann über die Angabe eines Bereichs in eckigen Klammern erreicht werden. Dabei ist der Index des ersten benötigten Zeichens sowie der Index des letzten benötigten Zeichens plus 1 anzugeben. Die Angabe `<firstname>[2:5]` gibt z.B. das dritte bis fünfte Zeichen des Vornamens zurück.

Das Anhängen von `:lower` oder `:upper` an den Attributnamen führt dazu, dass der Attributwert in Klein- oder Großschreibung umgewandelt wird, z.B. `<firstname:lower>`. Wird ein Modifikator wie `:lower` an das Ende des Feldes angehängt, wird der komplette Wert umgewandelt, z.B. `<lastname>@company.com<:lower>`.

Durch die Option `:umlauts` werden Sonderzeichen wie *è*, *ä* oder *ß* in entsprechende ASCII-Zeichen umgewandelt.

Durch die Option `:alphanum` werden alle nicht alphanumerischen Zeichen, wie ` oder # (Hash) entfernt. In der UCR Variable *directory/manager/templates/alphanum/whitelist* (Seite 305) können Zeichen definiert werden, die von dieser Option ignoriert werden. Zu beachten ist, dass wenn diese Option auf das ganze Feld angewendet wird, auch manuell gesetzte Zeichen entfernt werden. Zum Beispiel das @-Zeichen in der E-Mail-Adresse. Daher sollte man diese Option nur auf einzelne Attribute anwenden oder die Whitelist anpassen.

Die Optionen `:strip` oder `:trim` entfernen alle Leerzeichen am Anfang und Ende der Zeichenkette.

Optionen können auch kombiniert werden, z.B: `:umlauts,upper`.

6.8 Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos

Vorsicht: Bevor Sie diese Funktion verwenden, lesen Sie KB 14404 - Support-Artikel über die Aktivierung des lastbind Overlay-Moduls[28].

Das optionale lastbind Overlay-Modul[29] für OpenLDAP ermöglicht die Aufzeichnung des Zeitstempels der letzten erfolgreichen LDAP-Anmeldung im `authTimestamp` Attribut und kann z.B. zur Erkennung nicht genutzter Konten verwendet werden.

Das `lastbind` Overlay-Modul kann aktiviert werden, indem die Univention Configuration Registry Variable *ldap/overlay/lastbind* (Seite 309) auf `yes` gesetzt und der OpenLDAP-Server neu gestartet wird. Wenn das Modul auf einem UCS-Server aktiviert ist, wird der Zeitstempel einer erfolgreichen LDAP-Anmeldung eines Kontos, in das `authTimestamp` Attribut jenes Kontos geschrieben. Die Univention Configuration Registry Variable *ldap/overlay/lastbind/precision* (Seite 309) kann verwendet werden, um die Zeit in Sekunden zu konfigurieren, die vergehen muss, bevor das `authTimestamp` Attribut aktualisiert wird. Dies verhindert eine große Anzahl von Schreiboperationen, die die Leistung beeinträchtigen können.

Das `authTimestamp` Attribut kann nur auf dem LDAP-Server abgefragt werden, auf dem das `lastbind` Overlay-Modul aktiviert ist. Es wird nicht auf andere LDAP-Server repliziert. Aus diesem Grund kann das Skript `/usr/share/univention-ldap/univention_lastbind.py` ausgeführt werden, um den jüngsten `authTimestamp` Wert von allen erreichbaren LDAP-Servern in der UCS-Domäne zu sammeln und in das

[28] https://help.univention.com/t/14404
[29] https://manpages.ubuntu.com/manpages/xenial/man5/slapo-lastbind.5.html

erweiterte UDM Attribut `lastbind` eines Benutzers zu speichern. Das Skript kann aufgerufen werden, um das erweiterte Attribut `lastbind` eines oder aller Benutzer zu aktualisieren. Das erweiterte Attribut `lastbind` wird auf das LDAP-Attribut `univentionAuthTimestamp` abgebildet.

Eine Möglichkeit, das erweiterte Attribute `lastbind` aktuell zu halten, ist durch das Anlegen eines Cron-Jobs via UCR:

```
$ ucr set cron/update_lastbind_attribute/command='\
/usr/share/univention-ldap/univention_lastbind.py --allusers'\
  cron/update_lastbind_attribute/time='00 06 * * *'  # täglich um 06:00 Uhr.
```

Weitere Informationen über die Einstellung von Cron-Jobs über UCR können in *Definition eigener Cron-Jobs in Univention Configuration Registry* (Seite 173) gefunden werden.

6.9 Wiederverwendung von Benutzereigenschaften verhindern

Neu in Version 5.0-6-erratum-974: Seit UCS 5.0 erratum 974[30] unterstützt UCS Blocklisten, um die Wiederverwendung von Benutzer- oder Gruppeneigenschaftswerten zu verhindern.

Blocklisten ist ein Modul in UDM. Es ermöglicht die Konfiguration von Blocklisten für UDM Eigenschaften. Ändert oder entfernt ein Administrator oder eine Software eine UDM Eigenschaft an einem UDM Objekt, fügt die Blockliste automatisch einen Eintrag über diese Eigenschaft mit ihrem Wert in die Blockliste ein. Der Eintrag in der Blockliste verhindert, dass ein anderes UDM Objekt den gleichen Wert der UDM Eigenschaft verwenden kann. Blocklisten arbeiten auf der UDM Ebene.

Sie wollen zum Beispiel verhindern, dass UCS die Werte der UDM Eigenschaft `mailPrimaryAddress` der UDM Objekte *user* wiederverwendet. Sie konfigurieren eine Blockliste für die UDM Eigenschaft `mailPrimaryAddress`. Wenn Sie dann den Wert `chef@example.com` für die UDM Eigenschaft `mailPrimaryAddress` aus einem UDM Benutzerobjekt entfernen, erzeugt die UDM Blockliste einen Eintrag für diesen Wert. Wenn Sie den Wert von `james@example.com` auf `john@example.com` für die UDM Eigenschaft `mailPrimaryAddress` ändern, erzeugt die UDM Blockliste einen weiteren Eintrag für `james@example.com`.

UDM Blocklisten verhindern nun die Wiederverwendung der Werte `chef@example.com` und `james@example.com`. Sie können in anderen UDM Benutzerobjekten für die UDM Eigenschaft `mailPrimaryAddress` nicht mehr verwendet werden.

6.9.1 Aktivieren von Blocklisten

Bevor Sie die Blocklisten aktivieren können, müssen Sie zuerst die UCS Systeme, in denen Sie UDM Objekte verwalten, mindestens auf UCS 5.0 erratum 974[31] aktualisieren.

Zweitens müssen Sie die Univention Configuration Registry Variable *`directory/manager/blocklist/enabled`* (Seite 304) mit *`ucr set`* (Seite 163) auf allen UCS-Systemen, auf denen Sie UDM Objekte verwalten, auf `true` setzen.

[30] https://errata.software-univention.de/#/?erratum=5.0x974
[31] https://errata.software-univention.de/#/?erratum=5.0x974

6.9.2 Konfigurieren von Blocklisten

Sie können Blocklisteneinträge mit dem UMC-Modul *Blocklisten* oder über das Kommandozeilenwerkzeug **udm blocklists/list** erstellen, auflisten und entfernen.

Für jede Blockliste müssen Sie die folgenden Eigenschaften festlegen:

Name
: Gibt der Blockliste einen menschenlesbaren Namen für die spätere Identifizierung.

Aufbewahrungszeit
: Legt die Aufbewahrungszeit für Einträge in dieser Blockliste fest. Die Aufbewahrungszeit ist der Zeitraum, der ablaufen muss, um Einträge automatisch aus der Blockliste zu entfernen. Zum Beispiel `1m 20d`, was für einen Monat und zwanzig Tage steht.

Zu blockierende Eigenschaften
: Definiert die UDM Module und ihre Eigenschaften, deren Wiederverwendung die Blockliste verhindert.

Das folgende Beispiel für **udm blocklists/list** zeigt, wie man eine Blockliste über die Befehlszeile erstellt wird. Die Blockliste verhindert die Wiederverwendung der UDM Eigenschaft `mailPrimaryAddress` für `users/user` Objekte und die UDM Eigenschaft `mailAddress` für `groups/group` Objekte.

```
$ udm blocklists/list create \
  --set name=user-and-group-emails \
  --set retentionTime=40d \
  --append blockingProperties="users/user mailPrimaryAddress" \
  --append blockingProperties="groups/group mailAddress"
```

6.9.3 Einträge in der Blockliste verwalten

Sie können Blocklisteneinträge im UMC-Modul *Blocklisten* oder über das Kommandozeilenwerkzeug **udm blocklists/list** verwalten.

Wenn Sie Blocklisten aktiviert haben, erstellt UDM automatisch Einträge in der konfigurierten Blockliste, wenn Sie einen Wert aus einer UDM Eigenschaft eines UDM Objekts entfernen. UDM löscht abgelaufene Einträge automatisch aus der Blockliste.

Jeder Blocklisteneintrag hat die folgenden Eigenschaften:

Wert
: Ein SHA-256-Hash, der den Wert darstellt, den die Blockliste für die Wiederverwendung blockiert. Der Wert für die UDM Eigenschaft ist ein Klartextwert. Bevor UDM den Blocklisteneintrag erstellt, wird der Wert in Kleinbuchstaben umgewandelt. Alle groß- und kleingeschriebenen Varianten des Wertes stimmen dann mit dem Blocklisteneintrag überein, wenn er von UDM validiert wird.

Blockiert bis
: Der Zeitstempel, zu dem der Eintrag in der Blockliste abläuft. Er verwendet das GeneralizedTime-LDAP-Syntax[32] Format.

  Wenn UDM einen Blocklisteneintrag erstellt, nimmt es das aktuelle Datum und die aktuelle Uhrzeit, addiert die konfigurierte Aufbewahrungszeit der entsprechenden Blockliste und schreibt das Ergebnis nach *Blockiert bis*.

  Eine Änderung der Aufbewahrungszeit der Blockliste führt nicht zur Aktualisierung der Eigenschaft *Blockiert bis* des Blocklisteneintrags.

ID des Ursprungsobjekts
: Die ID des UDM Objekts, das den Blocklisteneintrag verursacht hat. Sie können weiterhin den Wert des Blocklisteneintrags für dieses UDM Objekt verwenden.

Wichtig: Wenn Sie die Einträge der Blockliste auflisten, erhalten Sie nur die Hashes der blockierten Werte.

[32] https://ldapwiki.com/wiki/Wiki.jsp?page=GeneralizedTime

Sie können jedoch nach dem Klartextwert eines bestimmten Eintrags suchen, z. B. wenn Sie diesen Eintrag löschen möchten.

```
$ udm blocklists/entry list
DN: cn=sha256:a859cd5964b6ac...,cn=emails,cn=blocklists
DN: cn=sha256:b859cd5964b6ac...,cn=emails,cn=blocklists
DN: cn=sha256:c859cd5964b6ac...,cn=emails,cn=blocklists

$ udm blocklists/entry list --filter value=blocked_email@example.com
DN: cn=sha256:c859cd5964b6ac...,cn=emails,cn=blocklists
```

6.9.4 Abgelaufene Blocklisteneinträge

Jeder Eintrag in einer Blockliste hat eine Eigenschaft *Blockiert bis*. Blocklisteneinträge laufen nach Ablauf dieses Zeitstempels ab. Ein Cron-Job auf dem Primary Directory Node löscht abgelaufene Blocklisteneinträge.

Sie können die Häufigkeit, mit der Cron den Job ausführt, mit dem Parameter Univention Configuration Registry Variable *directory/manager/blocklist/cleanup/cron* (Seite 304) konfigurieren. Die Protokolldatei `/var/log/univention/blocklist-clean-expired-entries.log` listet die abgelaufenen Einträge auf, die UDM gelöscht hat.

6.9.5 LDAP ACLs für Blocklisten

Standardmäßig kann jeder UCS Knoten in der Domäne und jedes Mitglied der Gruppe `Domain Admins` Blocklisteneinträge schreiben. Und jeder kann lesen. Sie können die Berechtigungen für den Primary Directory Node und den Backup Directory Nodes mit den folgenden Univention Configuration Registry Variablen konfigurieren:

- *ldap/database/internal/acl/blocklists/groups/read* (Seite 308)
- *ldap/database/internal/acl/blocklists/groups/write* (Seite 308)

Wenn Sie zum Beispiel einem Benutzer das Recht geben wollen, Einträge in der Blockliste zu löschen, der nicht Mitglied der Gruppe `Domain Admins` ist, müssen Sie eine Gruppe mit diesem Benutzer als Mitglied erstellen und den LDAP DN dieser Gruppe zu *ldap/database/internal/acl/blocklists/groups/write* (Seite 308) hinzufügen.

KAPITEL 7

Gruppenverwaltung

Berechtigungen werden in UCS überwiegend auf Basis von *Gruppen* unterschieden. Gruppen werden im LDAP gespeichert und sind somit auf allen Systemen identisch. Gruppen können nicht nur Benutzerkonten enthalten, sondern optional auch Rechnerkonten aufnehmen.

Auf jedem System gibt es darüber hinaus auch noch lokale Benutzergruppen, die vor allem für den Zugriff auf Hardware verwendet werden. Diese werden nicht durch das UCS Managementsystem verwaltet, sondern in der Datei `/etc/group` gespeichert.

Bemerkung: Die Gruppenverwaltung ist Teil von Univention Nubus in der *Directory Manager* Komponente. Weitere Informationen zu Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 2)

7.1 Zuordnung von Benutzergruppen

Die Zuordnung von Benutzern zu Gruppen erfolgt auf zwei Wegen:

- In der Benutzerverwaltung kann einem Benutzer eine Auswahl von Gruppen zugewiesen werden, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110).
- In der Gruppenverwaltung kann einer Gruppe eine Auswahl von Benutzern zugeordnet werden, siehe *Verwaltung von Gruppen über Univention Management Console Modul* (Seite 140).

7.2 Empfehlung für Definition von Gruppennamen

Ein sehr wichtiges und erforderliches Attribut für Gruppen ist der Gruppenname. Um Konflikte mit den verschiedenen Werkzeugen zu vermeiden, die Gruppen in UCS verarbeiten, berücksichtigen Sie die folgenden Empfehlungen für die Definition von Gruppennamen:

- Verwenden Sie für Gruppennamen nur Groß- und Kleinbuchstaben (`A-Za-z`), Ziffern (`0-9`), den Bindestrich (`-`) und Leerzeichen aus dem ASCII-Zeichensatz.
- Der Gruppenname beginnt mit einem Buchstaben aus dem ASCII-Zeichensatz. Das Leerzeichen ist weder als erstes, noch als letztes Zeichen erlaubt. Der Bindestrich als letztes Zeichen ist nicht erlaubt.
- In UCS hat der Gruppenname eine Länge von mindestens 4 und höchstens 20 Zeichen.

Die Empfehlung ergibt den folgenden regulären Ausdruck:

```
^[A-Za-z][A-Za-z0-9 -]{2,18}[A-Za-z0-9]$
```

Betrachten Sie die Empfehlung als Richtlinie und nicht als harte Regel und bedenken Sie mögliche Nebenwirkungen, wenn Sie Gruppennamen außerhalb der Empfehlung definieren.

7.3 Verwaltung von Gruppen über Univention Management Console Modul

Gruppen werden im UMC-Modul *Gruppen* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)).

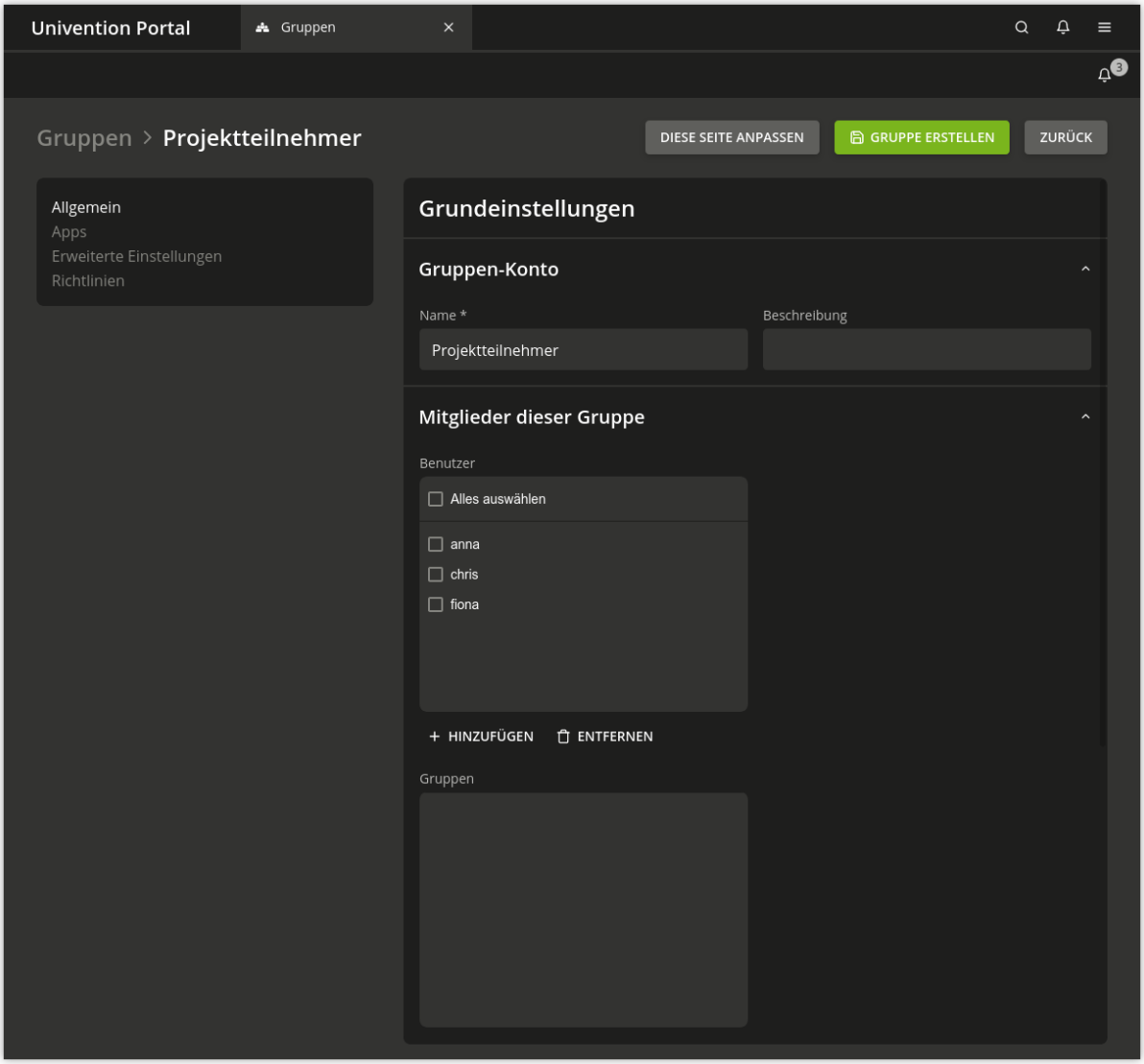


Abb. 7.1: Anlegen einer Gruppe im UMC-Modul

7.3.1 Gruppenmanagement Modul - Reiter Allgemein

Tab. 7.1: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Definiert den Namen der Gruppe. Für empfohlene Zeichen für den Gruppennamen, siehe *Empfehlung für Definition von Gruppennamen* (Seite 139). In der Grundeinstellung kann keine Gruppe mit dem Namen eines existierenden Benutzers angelegt werden. Wird die Univention Configuration Registry Variable `directory/manager/user_group/uniqueness` (Seite 305) auf `false` gesetzt, wird diese Prüfung aufgehoben.
Beschreibung	Hier kann eine beliebige Beschreibung für die Gruppe eingetragen werden.
Benutzer	In diesem Eingabefeld können Benutzer als Mitglieder in diese Gruppe aufgenommen werden.
Gruppen	In diesem Eingabefeld können Gruppen als Mitglieder in diese Gruppe aufgenommen werden (Gruppen in Gruppen).

7.3.2 Gruppenmanagement Modul - Reiter Erweiterte Einstellungen

Tab. 7.2: Reiter *Erweiterte Einstellungen*

Attribut	Beschreibung
Mail	Diese Optionen definieren eine Mailgruppe und sind in *Verwaltung von Mailgruppen* (Seite 274) dokumentiert.
Enthaltene Rechner	In diesem Feld können Rechner als Mitglieder in diese Gruppe aufgenommen werden.
Mitglied von	Hier kann diese Gruppe einer oder mehreren anderen Gruppen als Mitglied hinzugefügt werden (Gruppen in Gruppen).
Gruppen ID	Wenn der Gruppe eine bestimmte Gruppen-ID zugewiesen werden soll, kann die Gruppen-ID in diesem Eingabefeld eingetragen werden. Ansonsten wird der Gruppe automatisch die nächste freie Gruppen-ID zugeordnet. Sie kann nachträglich nicht geändert werden und wird beim Bearbeiten der Gruppe ausgegraut angezeigt. Als Gruppen-ID können ganze Zahlen zwischen 1000 und 59999 sowie zwischen 65536 und 1000000 frei vergeben werden.
Windows ▸ Relative ID	Die Relative ID (RID) ist der lokale Teil der Security ID (SID) und wird in Windows- und Samba-Domänen verwendet. Wenn der Gruppe eine bestimmte RID zugewiesen werden soll, kann sie in diesem Eingabefeld eingetragen werden. Ansonsten wird automatisch eine RID zugewiesen. Die RID kann nachträglich nicht geändert werden und wird beim Bearbeiten der Gruppe ausgegraut angezeigt. Die RIDs bis 1000 sind Standard-Gruppen und anderen speziellen Objekten vorbehalten. Bei Verwendung von Samba/AD wird die RID durch Samba generiert und kann nicht vorgegeben werden.
Windows ▸ Gruppentyp	Dieser Gruppentyp wird ausgewertet, wenn der Benutzer sich an einer Domäne auf Basis von Samba/AD anmeldet. Man unterscheidet zwischen drei Windows-Gruppentypen: **Domänengruppen** sind domänenweit bekannt. Neu erstellte Gruppen im UMC-Modul *Gruppen* sind standardmäßig von diesem Typ. **Lokale Gruppen** sind nur auf Windows-Servern von Bedeutung. Wird auf einem Windows-Server eine lokale Gruppe erstellt, ist sie nur dem Server bekannt und ist nicht domänenweit verfügbar. UCS hingegen unterscheidet nicht zwischen lokalen und globalen Gruppen. Von einer AD-Domäne übernommene lokale Gruppen werden in UCS wie globale Gruppen verwaltet. **Bekannte Gruppe** Unter diesem Gruppentyp werden von Samba- und Windows-Servern vorkonfigurierte Gruppen zusammengefasst, die in der Regel über besondere Berechtigungen verfügen, z.B. `Power Users`.
Windows ▸ AD Gruppentyp	Dieser Gruppentyp wird nur ausgewertet, wenn der Benutzer sich an einer Domäne auf Basis von Samba/AD anmeldet (das Active Directory-Domänendienste bereitstellt). Diese Gruppen sind in *Synchronisation von Active Directory-Gruppen bei Verwendung von Samba/AD* (Seite 144) beschrieben.
Windows ▸ Samba-Privilegien	Mit dieser Eingabemaske wird einer Gruppe Windows-Systemrechte zugewiesen, z.B. die Berechtigung einen Windows-Client in die Domäne zu joinen. Diese Funktionalität ist in *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110) dokumentiert.

7.3.3 Gruppenmanagement Modul - Reiter Optionseinstellungen

Diese Karteikarte steht nur beim Hinzufügen von Gruppen zur Verfügung, nicht aber beim Bearbeiten von Gruppen. Sie ermöglicht es, bestimmte LDAP-Objektklassen für die Gruppe abzuwählen. Die Eingabefelder für Attribute dieser Klassen können dann nicht ausgefüllt werden.

Tab. 7.3: Reiter *Optionen*

Attribut	Beschreibung
Samba-Gruppe	Dieses Auswahlkästchen gibt an, ob die Gruppe die Objektklasse `sambaGroupMapping` erhält.
POSIX-Gruppe	Dieses Auswahlkästchen gibt an, ob die Gruppe die Objektklasse `posixGroup` erhält.

7.4 Verschachtelte Gruppen mit Gruppen in Gruppen

UCS unterstützt die Verschachtelung von Gruppen (auch bekannt als „Gruppen in Gruppen“). Dies vereinfacht die Verwaltung der Gruppen: Werden in einer Domäne beispielsweise zwei Standorte verwaltet, können zwei Gruppen `Techniker Standort A` und `Techniker Standort B` gebildet werden, denen jeweils die Benutzerkonten der Standort-Techniker zugewiesen werden.

Um eine standortübergreifende Techniker-Gruppe zu bilden, reicht es dann aus, die Gruppen `Techniker Standort A` und `Techniker Standort B` als Mitglieder dieser Gruppe zu definieren.

Zyklische Abhängigkeiten von Gruppen in Gruppen werden erkannt und abgewiesen. Diese Prüfung kann durch die Univention Configuration Registry Variable *directory/manager/web/modules/groups/group/checks/circular_dependency* (Seite 305) deaktiviert werden. Auch bei direkten Gruppenänderungen ohne das UCS Managementsystem müssen zyklische Mitgliedschaften vermieden werden.

Die Auflösung der verschachtelten Gruppenmitgliedschaften erfolgt während der Expandierung des Gruppencaches (siehe *Lokaler Gruppencache* (Seite 143)) und ist somit für Applikationen transparent.

7.5 Lokaler Gruppencache

Aus dem LDAP aufgelöste Benutzer- und Rechnerinformationen werden durch den Name Server Cache Daemon (NSCD) zwischengespeichert, siehe *Name Service Cache Daemon* (Seite 173).

Die Zwischenspeicherung der Gruppen erfolgt seit UCS 3.1 aus Performance- und Stabilitätsgründen nicht mehr über den NSCD, sondern durch das NSS-Modul **`libnss-extrausers`**. Die Gruppeninformationen werden automatisch durch das Skript `/usr/lib/univention-pam/ldap-group-to-file.py` in die Datei `/var/lib/extrausers/group` exportiert und dort von dem NSS-Modul ausgelesen.

Der Export erfolgt in der Grundeinstellung einmal täglich durch einen Cron-Job und wird zusätzlich gestartet wenn der Univention Directory Listener 15 Sekunden inaktiv gewesen ist. Das Intervall für die Cron-Aktualisierung wird über die Univention Configuration Registry Variable *nss/group/cachefile/invalidate_interval* (Seite 313) in Cron-Syntax (siehe *Definition eigener Cron-Jobs in /etc/cron.d/* (Seite 172)) festgelegt. Das Listener-Modul kann über die Univention Configuration Registry Variable *nss/group/cachefile/invalidate_on_changes* (Seite 313) aktiviert/deaktiviert werden (`true`/`false`).

Während des Generierens der Gruppencache-Datei kann das Skript prüfen, ob die Gruppenmitglieder weiterhin im LDAP-Verzeichnis vorhanden sind. Werden für die Verwaltung der Verzeichnisdaten nicht ausschließlich UMC-Module eingesetzt, kann die zusätzliche Prüfung durch Setzen der Univention Configuration Registry Variable *nss/group/cachefile/check_member* (Seite 313) auf `true` aktiviert werden.

7.6 Synchronisation von Active Directory-Gruppen bei Verwendung von Samba/AD

Wird Samba/AD eingesetzt, werden die Gruppenmitgliedschaften zwischen dem Samba 4-Verzeichnisdienst und dem OpenLDAP-Verzeichnisdienst durch den Univention S4-Connector synchronisiert, d.h. jede Gruppe auf UCS-Seite ist einer Gruppe im Active Directory assoziiert. Allgemeine Hinweise zum Univention S4 Connector finden sich in *Univention S4 Connector* (Seite 179).

Einzige Ausnahme sind die *Pseudogruppen*, manchmal auch als Systemgruppen bezeichnet. Diese werden nur intern von Active Directory/Samba verwaltet, z.B. enthält die Gruppe `Authenticated Users` eine Liste aller aktuell an einem System angemeldeten Benutzer. Pseudogruppen sind im UCS-Verzeichnisdienst vorhanden; sie werden aber nicht durch den Univention S4 Connector synchronisiert und müssen normalerweise nicht bearbeitet werden. Dies betrifft die folgenden Gruppen:

- `Anonymous Logon`
- `Authenticated Users`
- `Batch`
- `Creator Group`
- `Creator Owner`
- `Dialup`
- `Digest Authentication`
- `Enterprise Domain Controllers`
- `Everyone`
- `IUSR`
- `Interactive`
- `Local Service`
- `NTLM Authentication`
- `Network Service`
- `Network`
- `Nobody`
- `Null Authority`
- `Other Organization`
- `Owner Rights`
- `Proxy`
- `Remote Interactive Logon`
- `Restricted`
- `SChannel Authentication`
- `Self`
- `Service`
- `System`
- `Terminal Server User`
- `This Organization`
- `World Authority`

Man unterscheidet in Active Directory/Samba zwischen den folgenden vier AD-Gruppentypen. Diese Gruppentypen können auf zwei Arten von Gruppen angewendet werden; *Sicherheitsgruppen* konfigurieren Berechtigungen (entsprechend den UCS-Gruppen), während *Verteilungsgruppen* für Mailverteiler genutzt werden:

Lokal
: *Lokale Gruppen* existieren immer nur lokal auf einem Rechner. Eine lokale Gruppe, die in Samba/AD angelegt wurde, wird durch den Univention S4 Connector synchronisiert und erscheint daher auch im UMC-Modul *Gruppen*. Es besteht aber keine Notwendigkeit lokale Gruppen im UMC-Modul anzulegen.

Global
: *Globale Gruppen* sind der Standardtyp für neu angelegte Gruppen im UMC-Modul *Gruppen*. Eine globale Gruppe gilt für eine Domäne, es können aber keine Konten anderer Domänen aufgenommen werden. Besteht eine Vertrauensstellung zu einer Domäne, werden die Gruppen dort angezeigt und es können Berechtigungen zugewiesen werden. Die aktuelle Version von UCS unterstützt allerdings weder mehrfache Domänen/Forests, noch von UCS ausgehende Vertrauensstellungen.

Domänenlokal
: *Domänenlokale Gruppen* können auch Mitglieder anderer Domänen aufnehmen (sofern zu diesen eine Vertrauenstellung besteht oder sie Teil eines Forests ist). Domänenlokale Gruppen werden aber nur in der eigenen Domäne angezeigt. Die aktuelle Version von UCS unterstützt allerdings weder mehrfache Domänen/Forests, noch von UCS ausgehende Vertrauensstellungen.

Universell
: *Universelle Gruppen* können Mitglieder aus allen Domänen aufnehmen und diese Mitglieder werden auch in allen Domänen eines Forests angezeigt. Diese Gruppen werden in einem separaten Segment des Verzeichnisdienstes gespeichert, dem sogenannten *Global Catalog*. Domänen-Forests werden aktuell von Samba/AD nicht unterstützt.

7.7 Overlay-Modul zur Anzeige der Gruppeninformationen an Benutzerobjekten

Im UCS-Verzeichnisdienst werden Gruppenmitgliedschaften nur an den Gruppenobjekten und nicht am jeweiligen Benutzerobjekt gespeichert. Einige Applikationen erwarten jedoch die Gruppenmitgliedschaften an den Benutzerobjekten (z.B. im Attribut `memberOf`). Durch ein optionales Overlay-Modul im LDAP-Server können diese Attribute automatisch anhand der Gruppeninformationen angezeigt werden. Die zusätzlichen Attribute werden nicht in das LDAP geschrieben, sondern bei einer Anfrage durch das Overlay-Modul ermittelt und angezeigt.

Vorsicht: Bevor Sie diese Funktion verwenden, lesen Sie bitte KB 6439 - memberOf attribute: Group memberships of user and computer objects[33] (Englisch) über die Aktivierung des `memberOf` Overlay-Moduls.

Dazu muss auf allen LDAP-Servern das Paket **`univention-ldap-overlay-memberof`** installiert werden. Anschließend muss **`/usr/share/univention-ldap-overlay-memberof/univention-update-memberof`** auf allen Servern aufgerufen werden.

In der Grundeinstellung wird das Benutzerattribut `memberOf` dargestellt. Mit der Univention Configuration Registry Variable *`ldap/overlay/memberof/memberof`* (Seite 309) kann auch ein anderes Attribut konfiguriert werden.

[33] https://help.univention.com/t/6439

KAPITEL 8

Rechnerverwaltung

8.1 Verwaltung der Rechnerkonten über Univention Management Console Modul

Alle UCS-, Linux- und Windowssysteme innerhalb einer UCS-Domäne verfügen über ein Rechner-Domänenkonto, mit dem sich die Systeme untereinander authentifizieren und mit dem sie auf das LDAP-Verzeichnis zugreifen.

Das Rechnerkonto wird in der Regel automatisch beim Join des Systems zur UCS-Domäne angelegt (siehe *Domänenbeitritt* (Seite 30)), das Rechnerkonto kann jedoch auch vor dem Domänenbeitritt angelegt werden.

Das Passwort für das Rechnerkonto wird beim Domänenbeitritt automatisch erzeugt und in der Datei `/etc/machine.secret` gespeichert. Das Passwort umfasst in der Grundeinstellung 20 Zeichen (konfigurierbar über die Univention Configuration Registry Variable *machine/password/length* (Seite 310)). Das Passwort wird in festen Intervallen automatisch neu generiert (in der Grundeinstellung 21 Tage, konfigurierbar über die Univention Configuration Registry Variable *server/password/interval* (Seite 317)). Die Passwortrotation kann über die Variable *server/password/change* (Seite 317) auch deaktiviert werden.

Für jede Systemrolle existiert ein eigenständiger Rechnerobjekttyp. Weitergehende Hinweise zu den einzelnen Systemrollen finden sich in *UCS-Systemrollen* (Seite 35).

Rechnerkonten werden im UMC-Modul *Rechner* verwaltet.

In der Grundeinstellung wird zum Anlegen eines Rechners ein vereinfachter Assistent angezeigt, der nur die wichtigsten Einstellungen abfragt. Durch einen Klick auf *Erweitert* werden alle Attribute angezeigt. Ist dem ausgewählten Netzwerk-Objekt (siehe *Netzwerk-Objekte* (Seite 219)) eine DNS-Forward-Zone und/oder eine DNS-Reverse-Zone zugeordnet (siehe *Verwaltung von DNS-Daten mit BIND* (Seite 221)), wird für den Rechner automatisch ein Host-Record und/oder Pointer-Record angelegt. Ist für das Netzwerk-Objekt ein DHCP-Service konfiguriert und eine MAC-Adresse angegeben, wird ein DHCP-Rechner-Eintrag angelegt (siehe *IP-Vergabe über DHCP* (Seite 228)).

Der vereinfachte Assistent kann für alle Systemrollen deaktiviert werden, indem die Univention Configuration Registry Variable *directory/manager/web/modules/computers/computer/wizard/disabled* (Seite 305) auf `true` gesetzt wird.

Abb. 8.1: Anlegen eines Rechners im UMC-Modul

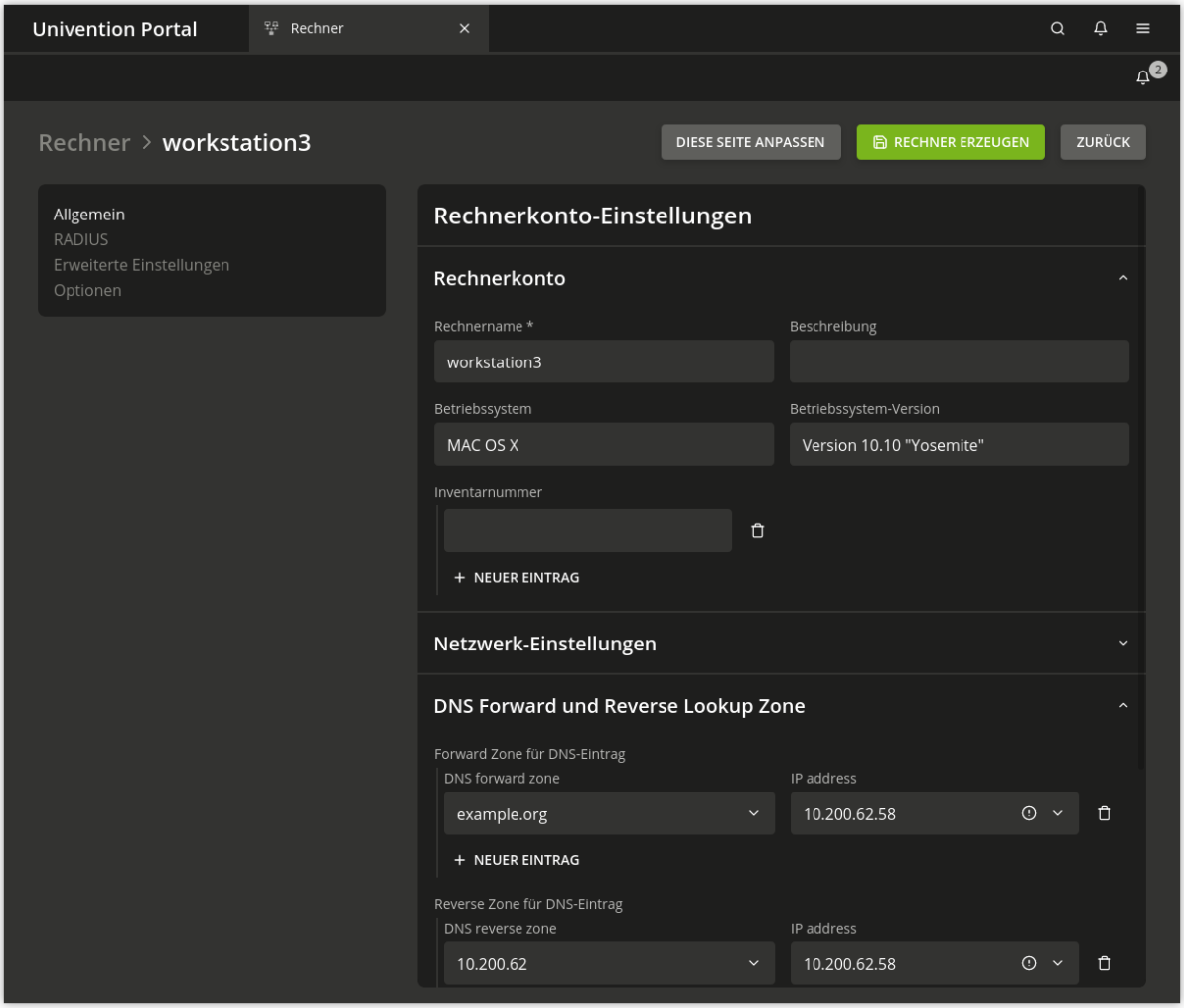


Abb. 8.2: Erweiterte Rechneransicht

8.1.1 Modul Rechnerverwaltung - Reiter Allgemein

Tab. 8.1: Reiter *Allgemein*

Attribut	Beschreibung
Name	In dieses Eingabefeld muss der Rechnername eingetragen werden. Um die Kompatibilität mit verschiedenen Betriebssystemen und Diensten zu gewährleisten, sollten Rechnernamen ausschließlich die Buchstaben *a* bis *z* in Kleinschreibung, Zahlen, Bindestriche und Unterstriche enthalten. Umlaute und Sonderzeichen sind nicht erlaubt. Der Punkt wird als Trennzeichen zwischen den einzelnen Bestandteilen eines voll qualifizierten Domänennamens interpretiert und darf deswegen nicht innerhalb des Rechnernamens verwendet werden. Rechnernamen sollten mit einem Buchstaben beginnen. Microsoft Windows akzeptiert nur Rechnernamen mit maximal 13 Zeichen, so dass man sich bei Rechnernamen grundsätzlich auf 13 Zeichen beschränken sollte, sofern nicht ausgeschlossen ist, dass Microsoft Windows zum Einsatz kommen wird. Der Rechnername kann nach dem Anlegen nur bei den Systemrollen *Windows Workstation/Server*, *macOS Client* und *IP-Client* verändert werden.
Beschreibung	Für den Rechner kann in diesem Eingabefeld eine beliebige Beschreibung hinterlegt werden.
Inventarnummer	Hier können Inventarnummern für Rechner hinterlegt werden.
Netzwerk	Der Rechner kann einem bereits angelegten Netzwerk-Objekt zugeordnet werden. Hinweise zur IP-Konfiguration finden sich in *Netzwerk-Objekte* (Seite 219).
MAC-Adresse	An dieser Stelle kann die MAC-Adresse des Rechners eingetragen werden, z.B. `2e:44:56:3f:12:32`. Soll der Rechner einen DHCP-Eintrag erhalten, ist die Angabe der MAC-Adresse zwingend erforderlich.
IP-Adresse	Hier können feste IP-Adressen für den Rechner eingegeben werden. Weitere Hinweise zur IP-Konfiguration finden sich in *Netzwerk-Objekte* (Seite 219). Wenn auf der Karteikarte *Allgemein* ein Netzwerk ausgewählt wurde, wird die IP-Adresse, die dem Rechner aus dem Netzwerk automatisch zugewiesen wurde, hier angezeigt. Eine hier (also im LDAP-Verzeichnis) eingetragene IP-Adresse kann dem Rechner nur über DHCP zugewiesen werden. Sollte kein DHCP-Server verwendet werden, so muss die IP-Adresse auch lokal auf dem Rechner konfiguriert werden, siehe *Netzwerk Konfiguration* (Seite 155). Werden die eingetragenen IP-Adressen eines Rechners ohne Wechsel der DNS-Zonen geändert, werden diese im Rechner-Objekt und - soweit vorhanden - auch automatisch in den DNS-Einträgen in der Forward und Reverse Lookup Zone geändert. Falls die IP-Adresse des Rechners noch an anderen Stellen eingetragen wurde, müssen diese Einträge manuell geändert werden! Wurde beispielsweise in einer DHCP-Boot-Richtlinie nicht der Name des Boot-Servers, sondern seine IP-Adresse dort eingetragen, muss diese IP-Adresse manuell durch das Bearbeiten der Richtlinie angepasst werden.
Forward-Zone für DNS-Eintrag	Die DNS-Forward-Zone, in die der Rechner eingetragen wird. Die Zone dient der Auflösung des Rechnernamens in die zugewiesene IP-Adresse. Hinweise zur IP-Konfiguration finden sich in *Netzwerk-Objekte* (Seite 219).
Reverse-Zone für DNS-Eintrag	Die DNS-Reverse-Zone, in die der Rechner eingetragen wird. Mit der Zone wird die IP-Adresse des Rechners in einen Rechnernamen aufgelöst. Hinweise zur IP-Konfiguration finden sich in *Netzwerk-Objekte* (Seite 219).
Service für DHCP-Eintrag	Wenn ein Rechner seine IP-Adresse über DHCP beziehen soll, muss hier ein DHCP-Service zugeordnet werden. Hinweise zur IP-Konfiguration finden sich in *Netzwerk-Objekte* (Seite 219). Bei der Zuweisung muss darauf geachtet werden, dass die DHCP-Server des DHCP-Service-Objekts für das physikalische Netzwerk zuständig sind. Wurde auf der Karteikarte *Allgemein* ein Netzwerk ausgewählt, wird automatisch ein für das Netzwerk passender Eintrag hinzugefügt, der nachträglich manuell angepasst werden kann.

8.1.2 Modul Rechnerverwaltung - Reiter Konto

Tab. 8.2: Reiter *Konto* (erweiterte Einstellungen)

Attribut	Beschreibung
Passwort	Das Passwort des Rechnerkontos wird in der Regel automatisch erstellt und rotiert. Für Sonderfälle wie die Einbindung externer Systeme kann es in diesem Feld auch explizit konfiguriert werden. Dasselbe Passwort muss dann auch lokal auf dem Rechner in die Datei `/etc/machine.secret` eingetragen werden.
Primäre Gruppe	In diesem Auswahlfeld kann die primäre Gruppe des Rechners selektiert werden. Das ist nur notwendig, wenn von den automatisch eingestellten Vorgabewerten abgewichen werden soll. Der Vorgabewert für einen Primary Directory Node oder Backup Directory Node lautet `DC Backup Hosts`, für einen Replica Directory Node `DC Slave Hosts` und für Managed Nodes `Computers`.

8.1.3 Modul Rechnerverwaltung - Reiter Unix-Konto

Tab. 8.3: Reiter *Unix-Konto* (erweiterte Einstellungen)

Attribut	Beschreibung
UNIX Heimatverzeichnis (*)	In diesem Eingabefeld kann ein abweichendes Heimatverzeichnis für das Rechner-Konto eingetragen werden. Der automatisch eingestellte Vorgabewert für das Heimatverzeichnis lautet `/dev/null`.
Login Shell	Falls eine vom Vorgabewert abweichende Login-Shell für das Rechner-Konto verwendet werden soll, kann die Login-Shell in diesem Eingabefeld manuell angepasst werden. Der automatisch eingestellte Vorgabewert sieht `/bin/sh` als Login-Shell vor.

8.1.4 Modul Rechnerverwaltung - Reiter Dienste

Tab. 8.4: Reiter *Dienste* (erweiterte Einstellungen)

Attribut	Beschreibung
Dienst	Mit einem Dienst-Objekt können Applikationen oder Dienste feststellen, ob auf einem Rechner oder generell in der Domäne ein Dienst verfügbar ist.

Bemerkung: Der Reiter *Dienste* wird nur auf UCS-Systemrollen angezeigt.

8.1.5 Modul Rechnerverwaltung - Reiter (Re)installation

Dieser Reiter wird für den Univention Net Installer verwendet, siehe *Extended installation documentation* [6].

8.1.6 Modul Rechnerverwaltung - Reiter DNS-Alias

Tab. 8.5: Reiter *DNS Alias* (Erweiterte Einstellungen)

Attribut	Beschreibung
Zone für DNS-Alias	Wenn für den Rechner im Feld *Forward Lookup Zone für DNS-Eintrag* ein Zoneneintrag zur Vorwärtsauflösung eingerichtet wurde, können hier zusätzlich Alias-Einträge konfiguriert werden, über die der Rechner erreichbar ist.

8.1.7 Modul Rechnerverwaltung - Reiter Dienste

Tab. 8.6: Reiter *Alerts* (erweiterte Einstellungen)

Attribut	Beschreibung
Überwachungsalarme zuweisen	Legt fest, welche Monitoring Alert Prüfungen für diesen Rechner ausgeführt werden, siehe *Konfiguration der Alarme* (Seite 297).

8.1.8 Modul Rechnerverwaltung - Reiter Gruppen

In diesem Reiter kann der Rechner in verschiedene Gruppen aufgenommen werden.

8.1.9 Modul Rechnerverwaltung - Reiter Optionen

Der Reiter ermöglicht es, einzelne LDAP-Objektklassen für den Rechner zu konfigurieren. Die Eingabefelder für Attribute abgewählter Objektklassen werden dann nicht angezeigt. Nicht alle Objektklassen können nachträglich verändert werden.

Tab. 8.7: Reiter *(Optionen)*

Attribut	Beschreibung
Kerberos Prinzipal	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklassen `krb5Principal` und `krb5KDCEntry` nicht.
POSIX Konto	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklasse `posixAccount` nicht.
Samba-Konto	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklasse `sambaSamAccount` nicht.

8.1.10 Integration von Ubuntu-Clients

Ubuntu-Clients können mit einer eigenen Rechnerrolle im UMC-Modul *Rechner* verwaltet werden. Die Netzwerkeigenschaften für DNS/DHCP können dabei ebenfalls dort verwaltet werden.

Die Anwendung von Richtlinien wird nicht unterstützt.

Auf den Ubuntu-Systemen müssen einige Konfigurationsanpassungen vorgenommen werden, die in *Extended domain services documentation* [2] beschrieben sind.

8.2 Konfiguration von Hardware und Treibern

8.2.1 Verfügbare Kernel-Varianten

Der Standard-Kernel in UCS 5.0 basiert auf dem Linux-Kernel 4.19. Prinzipiell sind drei verschiedene Arten von Kernel-Paketen zu unterscheiden:

- Ein *Kernel-Image-Paket* stellt einen lauffähigen Kernel bereit, der installiert und gestartet werden kann.
- Ein *Kernel-Source-Paket* stellt den Quellcode für einen Kernel bereit. Aus diesem kann beispielsweise ein angepasster Kernel erstellt werden, indem Funktionen aktiviert oder deaktiviert werden können.
- Ein *Kernel-Header-Paket* stellt Schnittstellen-Informationen bereit, die von externen Paketen benötigt werden, wenn diese auf Kernel-Funktionen zugreifen müssen. Sie werden typischerweise zum Übersetzen externer Kernel-Treiber benötigt.

Im Regelfall ist für den Betrieb eines UCS-Systems nur die Installation eines Kernel-Image-Paketes notwendig.

Mehrere Kernel-Varianten können parallel installiert sein. Dies stellt sicher, dass im Fehlerfall immer auf eine ältere Variante zurückgegriffen werden kann. Um ein System trotzdem immer auf dem jeweils aktuellen Stand halten zu können, werden sogenannte Meta-Pakete bereit gestellt, die immer auf die aktuell für UCS empfohlene Kernel-Version verweisen und diese im Update-Fall jeweils nachinstallieren.

8.2.2 Treiber-Management / Kernel-Module

Der Boot-Prozess erfolgt zweistufig unter Verwendung einer Initial RAM Disk (kurz *initrd*). Diese besteht aus einem Archiv mit weiteren Treibern und Programmen.

Der Boot-Manager GRUB (siehe *GRUB Boot-Manager* (Seite 154)) lädt den Kernel und die *initrd* in den Arbeitsspeicher, wo das *initrd*-Archiv entpackt und als temporäres Root-Dateisystem gemountet wird. Aus diesem wird dann das tatsächliche Root-Dateisystem eingebunden, woraufhin abschließend das temporäre Archiv wieder entfernt und der Systemstart eingeleitet wird.

Die zu verwendenden Treiber werden beim Systemstart automatisch erkannt und durch den Device Manager **udev** geladen. Dabei werden außerdem die notwendigen System-Verknüpfungen unter `/dev/` angelegt. Wenn Treiber nicht erkannt werden (was vorkommen kann, wenn keine entsprechenden Hardware-IDs registriert sind oder Hardware verwendet wird, die nicht automatisch erkannt werden kann, etwa ISA-Steckkarten), so können zu ladende Kernel-Module durch die Univention Configuration Registry Variable *kernel/modules* (Seite 308) hinzugefügt werden. Soll mehr als ein Kernel-Modul geladen werden, so müssen diese durch ein Semikolon voneinander getrennt werden. Mit der Univention Configuration Registry Variable *kernel/blacklist* (Seite 308) kann eine Liste von einem oder mehreren Kernel-Modulen konfiguriert werden, für die das automatische Laden verhindert wird. Mehrere Einträge müssen ebenfalls durch ein Semikolon getrennt werden.

Im Gegensatz zu anderen Betriebssystemen liefert der Linux-Kernel (von wenigen Ausnahmen abgesehen) alle Treiber für Komponenten aus einer Hand. Im Regelfall ist es deshalb nicht notwendig Treiber aus externen Quellen nachzuinstallieren.

Wenn doch externe Treiber oder Kernelmodule benötigt werden, können diese über *Dynamic Kernel Module Support* (DKMS) eingebunden werden. Es stellt eine standardisierte Schnittstelle für Kernelquellen bereit und erlaubt es, Module automatisch für jeden installierten Kernel zu übersetzen. Dazu müssen neben dem Paket **dkms** auch die

Kernel-Header-Pakete **linux-headers-amd64** für die gewünschten Kernel installiert werden. Zu beachten ist, dass nicht alle externen Kernelmodule mit allen Kernel kompatibel sind.

8.2.3 GRUB Boot-Manager

Als Boot-Manager wird in Univention Corporate Server GNU GRUB 2 verwendet. GRUB stellt ein Auswahlmenü bereit, aus dem eine zu bootende Linux-Kernel-Variante oder ein weiteres Betriebssystem ausgewählt werden kann. GRUB kann auch direkt auf Dateisysteme zugreifen, so dass im Fehlerfall etwa ein abweichender Kernel geladen werden kann.

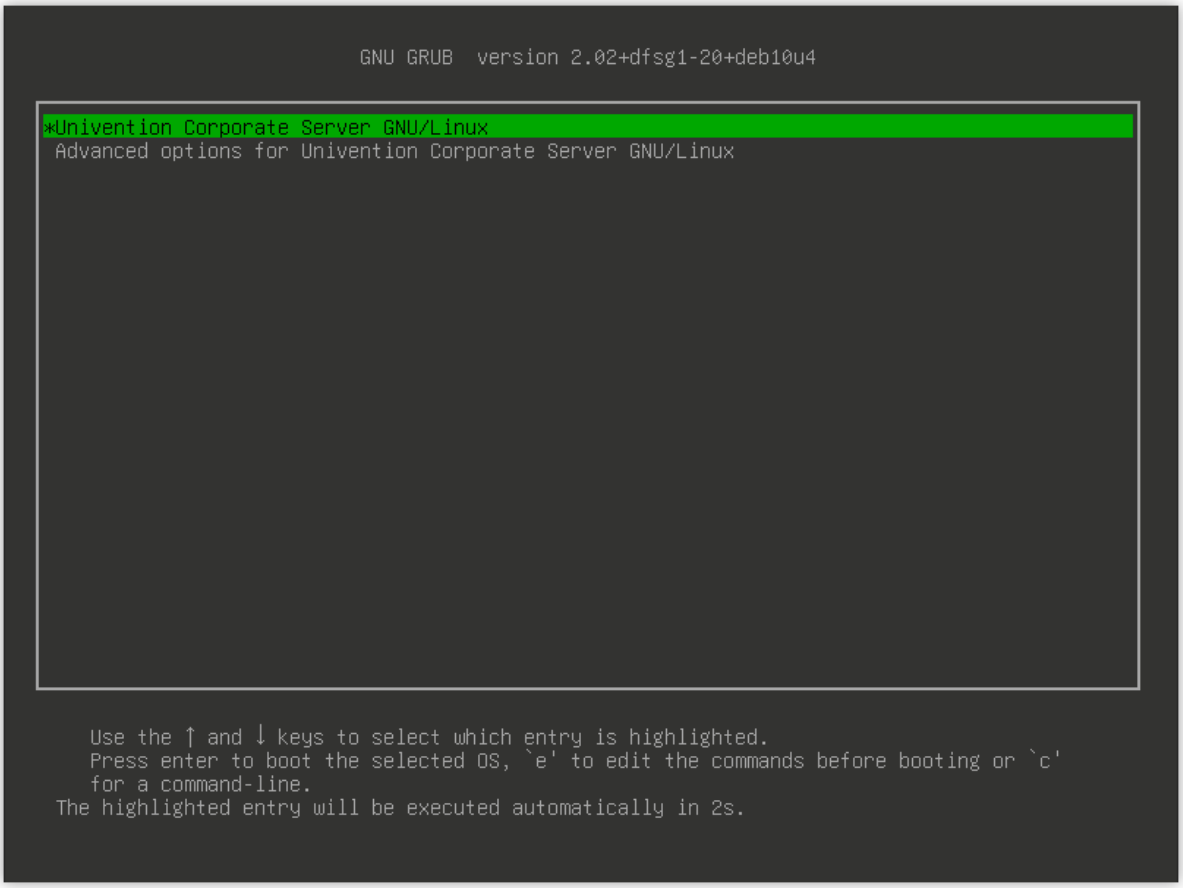


Abb. 8.3: GRUB-Auswahlmenü

GRUB wird in einem zweistufigen Verfahren geladen: in den Master Boot Record der Festplatte wird der Stage 1-Loader geschrieben, der auf die Daten der Stage 2 verweist, welche den Großteil des übrigen Boot-Vorgangs übernimmt.

Die Auswahl der zu startenden Kernel im Boot-Menü wird in der Datei `/boot/grub/grub.cfg` abgelegt. Diese Datei wird automatisch generiert, es stehen alle installierten Kernel-Pakete zur Auswahl. Durch Auswahl der Option *Memory test* kann das Speicher-Testprogramm **Memtest86+** gestartet werden, das Konsistenzprüfungen auf dem Arbeitsspeicher durchführt.

Standardmäßig wird fünf Sekunden auf die Auswahl des zu bootenden Kernels gewartet. Durch die Univention Configuration Registry Variable *grub/timeout* (Seite 307) kann ein abweichender Wert in Sekunden konfiguriert werden.

In der Grundeinstellung wird in einen `800x600` Pixel großen Bildschirm unter 16 Bit Farbtiefe gewechselt. Durch die Univention Configuration Registry Variable *grub/gfxmode* (Seite 307) kann ein anderer Modus ausgewählt werden. Es werden nur Auflösungen unterstützt, die über VESA BIOS Extentions gesetzt werden können. Eine Lis-

te der verfügbaren Modi findet sich unter VESA BIOS Extensions[34]. Die Eingabe erfolgt im Format *HORIZONTAL*x*VERTIKAL*@*FARBTIEFEBIT*, also z.B. `1024x768@16`.

Kernel-Optionen für die gestarteten Linux-Kernel können mit der Univention Configuration Registry Variable *grub/append* (Seite 307) übergeben werden. Mit der *grub/xenhopt* (Seite 307) können Optionen an den Xen-Hypervisor übergeben werden.

Die grafische Darstellung während des Bootvorgangs - der sogenannte Splash-Screen - kann durch Setzen der Univention Configuration Registry Variable *grub/bootsplash* (Seite 307) auf `nosplash` deaktiviert werden.

8.2.4 Netzwerk Konfiguration

Die Konfiguration von Netzwerk-Interfaces kann über das UMC-Modul *Netzwerk-Einstellungen* angepasst werden.

Die Konfiguration wird in Univention Configuration Registry-Variablen gespeichert, die auch direkt gesetzt werden können. Die Variablen sind in den einzelnen Abschnitten aufgeführt.

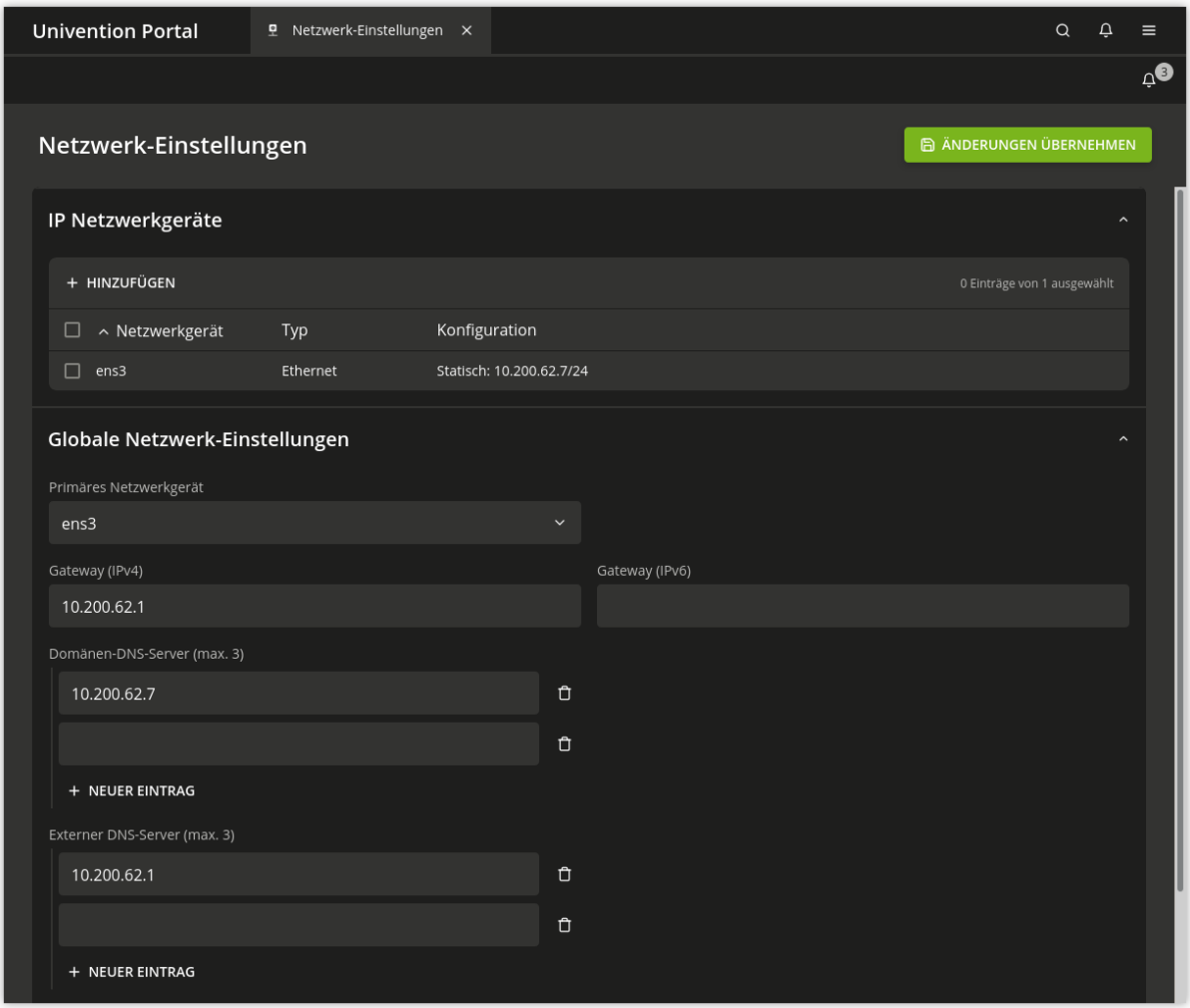


Abb. 8.4: Konfiguration der Netzwerkeinstellungen

Unter *IPv4-Netzwerkgeräte* und *IPv6-Netzwerkgeräte* werden alle im System verfügbaren Netzwerkkarten aufgeführt (es werden nur Netzwerkinterfaces im Schema `ethX` dargestellt).

Netzwerkschnittstellen können für IPv4 und/oder IPv6 konfiguriert werden. IPv4-Adressen haben 32 Bit Länge und werden in der Regel in vier Blöcken in Dezimalschreibweise dargestellt (z.B. `192.0.2.10`),

[34] https://de.wikipedia.org/wiki/VESA_BIOS_Extension

während IPv6-Adressen vier Mal so lang sind und typischerweise hexadezimal dargestellt werden (z.B. `2001:0DB8:FE29:DE27:0000:0000:0000:0000`).

Konfiguration von IPv4-Adressen

Wenn die Option *Dynamisch (DHCP)* nicht gewählt wurde, muss die IP-Adresse eingegeben werden, die an die Netzwerkkarte gebunden werden soll. Zusätzlich zur *IPv4-Adresse* muss die *Netzmaske* angegeben werden. Mit *DHCP-Anfrage* kann eine Adresse von einem DHCP-Server abgefragt werden. Sofern die Option *Dynamisch (DHCP)* nicht aktiviert wird, werden die aus der DHCP-Anfrage erhaltenen Werte dann statisch konfiguriert.

Auch Server-Systeme können per DHCP konfiguriert werden. Dies ist z.B. bei einigen Cloud-Anbietern notwendig. Schlägt die Vergabe einer IP-Adresse für einen Server fehl, wird ersatzweise eine zufällige Link-Local-Adresse (`169.254.x.y`) konfiguriert.

Die über DHCP erhaltene Adresse wird für UCS-Serversysteme auch in das LDAP-Verzeichnis geschrieben.

Bemerkung: Nicht alle Dienste (z.B. DNS-Server) sind für eine Verwendung auf einem DHCP-basierten Server geeignet.

UCR Variablen:

- *interfaces/ethX/address* (Seite 307)
- *interfaces/ethX/netmask* (Seite 307)
- *interfaces/ethX/type* (Seite 307)
- *gateway* (Seite 306)

Neben den physischen Interfaces können auch zusätzliche virtuelle Interfaces in der Form *interfaces/ethX_Y/setting* (Seite 307) definiert werden.

Konfiguration von IPv6-Adressen

Die IPv6-Adresse kann auf zwei Arten konfiguriert werden: Bei der *Automatischen Konfiguration (SLAAC)* kommt Stateless Address Autoconfiguration (SLAAC) zum Einsatz. Dabei wird die IP-Adresse von den Routern des lokalen Netzsegmentes zugewiesen. Alternativ kann die Adresse auch durch Angabe von *IPv6-Adresse* und *IPv6-Präfix* statisch konfiguriert werden.

Im Gegensatz zu DHCP wird bei SLAAC keine Zuweisung von weitergehenden Daten wie dem zu verwendenden DNS-Server durchgeführt. Hierfür gibt es mit DHCPv6 ein Zusatzprotokoll, das bei der dynamischen Zuweisung aber nicht zum Einsatz kommt. Eine Netzwerkkarte kann verschiedene IPv6-Adressen bedienen. Der *Bezeichner* ist ein eindeutiger Name für einzelne Adressen. Die Haupt-Adresse verwendet immer den Bezeichner *default*, für alle anderen Adressen können funktionale Bezeichner vergeben werden, z.B. `Interface-Mailserver`.

UCR Variablen:

- *interfaces/ethX/ipv6/address* (Seite 307)
- *interfaces/ethX/ipv6/prefix* (Seite 307),
- *interfaces/ethX/ipv6/acceptRA* (Seite 307) aktiviert SLAAC

Unter *Globale Netzwerk-Einstellungen* können weitere netzwerkbezogene Einstellungen vorgenommen werden.

Unter *Gateway (IPv4)* und *Gateway (IPv6)* können die für die IP-Adresse im Subnetz eingesetzten Standard-Gateways für IPv4 und IPv6 eingegeben werden. Für IPv6 ist die Angabe eines Gateways nicht erforderlich, wird jedoch empfohlen. Ein hier konfiguriertes IPv6-Gateway hat Vorrang vor Router Advertisements, die ansonsten die Route ändern könnten.

UCR Variablen:

- *ipv6/gateway* (Seite 307)

Konfiguration der Nameserver

Zwei Typen von DNS-Servern werden unterschieden:

Externer DNS Server
Ein *externer DNS-Server* wird für die Auflösung von Rechnernamen und Adressen außerhalb der UCS-Domäne verwendet, z.B. `univention.de`. Dies ist typischerweise ein Nameserver, der vom Internet Provider betrieben wird.

Domänen DNS Server
Ein *Domänen-DNS-Server* ist ein lokaler Nameserver der UCS-Domäne. Dort werden in der Regel die Rechnernamen und IP-Adressen der UCS-Domäne verwaltet. Wird eine Adresse im lokalen Datenbestand nicht aufgefunden, wird automatisch ein externer DNS-Server angefragt. Die DNS-Daten werden im LDAP-Verzeichnisdienst gespeichert, d.h. alle Domänen-DNS-Server liefern identische Daten aus.

Auf den Systemrollen Primary Directory Node, Backup Directory Node und Replica Directory Node läuft ein lokaler DNS-Server. Hier kann durch Angabe von *Domänen-DNS-Server* konfiguriert werden, welcher Server primär für die Namensauflösung verwendet wird.

UCR Variablen:

- *nameserver1* (Seite 313) bis *nameserver3* (Seite 313)
- *dns/forwarder1* (Seite 305) bis *dns/forwarder3* (Seite 305),

Bridges, Bonding, VLANs

UCS unterstützt komplexe Netzwerk-Konfigurationen mit Bridges, Bonding und VLAN-Netzen:

- Bridges werden oft von Virtualisierungslösungen verwendet, um virtualisierte Netzwerkkarten einer virtuellen Maschine mit der physischen Netzwerkkarte des Virtualisierungsservers zu verbinden.
- Bonding erhöht die Ausfallsicherheit, in dem mehrere physikalische Netzwerkkarten für den Zugriff auf ein Netzwerk gebündelt werden.
- VLANs können verwendet werden um den Netzwerkverkehr in einem physikalischen Netzwerk logisch auf ein oder mehrere virtuelle Unternetze aufzuteilen.

Konfiguration von Bridging

Der häufigste Anwendungsfall für *Bridging* ist die gemeinsame Nutzung einer physischen Netzwerkkarte durch eine oder mehrere virtuelle Maschinen. Anstatt eine Netzwerkkarte für jede virtuelle Maschine und den Virtualisierungsserver selbst zu verwenden, werden alle System durch einen gemeinsamen Uplink angebunden. Eine Bridge kann mit einem in Software realisierten Switch verglichen werden, über den einzelne Hosts miteinander verbunden werden. Die verwendete Hardware-Netzwerkkarte wird als *Bridge Port* bezeichnet.

Um eine Bridge zu konfigurieren muss unter *Hinzufügen* als *Netzwerkgerätetyp* `Bridge` ausgewählt werden. Der *Name des neuen Bridge-Netzwerkgerätes* kann beliebig gewählt werden. Anschließend muss auf *Weiter* geklickt werden.

Unter *Bridge ports* kann die physische Netzwerkkarte ausgewählt werden, die den Uplink darstellt. Im typischen Anwendungsfall der Anbindung virtueller Maschinen über nur eine Netzwerkkarte kann keine Schleife auftreten. Wird die Bridge zur Verbindung zweier Netzwerkkarten verwendet, wird das Spanning Tree Protocol (STP) zur Vermeidung von Netzwerkschleifen eingesetzt. Der Linux-Kernel implementiert lediglich STP, nicht die Varianten Rapid STP oder Multiple STP.

Die Einstellung *Forwarding delay* konfiguriert die Wartezeit in Sekunden, während der bei Aufbau einer Verbindung durch STP Informationen über die Netzwerktopologie gesammelt werden. Wird die Bridge zur Anbindung virtueller Maschinen über eine physische Netzwerkkarte verwendet, sollte STP dann deaktiviert werden, in dem der Wert auf `0` gesetzt wird. Ansonsten kann es zu Problemen bei der Verwendung von DHCP führen, da die während der Wartezeit versendeten Pakete nicht weitergeleitet werden.

Über das Eingabefeld *Weitere Geräteoptionen* können beliebige weitere Bridge-Parameter konfiguriert werden. Dies ist nur in Ausnahmefällen nötig, eine Übersicht der möglichen Einstellungen findet sich in der Manpage `bridge-utils-interfaces(5)`.

Nach einem Klick auf *Weiter* kann der Bridge optional eine IP-Adresse zugewiesen werden. Diese kann dann auch als Netzwerkinterface auf dem Virtualisierungshost verwendet werden. Die Einstellungsmöglichkeiten sind dieselben wie in *Konfiguration von IPv4-Adressen* (Seite 156) und *Konfiguration von IPv6-Adressen* (Seite 156) beschrieben.

Konfiguration von Bonding

Mit *Bonding* können zwei (oder mehr) physische Netzwerkkarten zur Erhöhung des Durchsatzes oder zur Verbesserung der Redundanz in Failoverszenarien gebündelt werden.

Um ein Bonding zu konfigurieren muss unter *Hinzufügen* als *Netzwerkgerätetyp* `Kanalbündelung (Bonding)` ausgewählt werden. Der *Name des neuen Bonding-Netzwerkgerätes* kann beliebig gewählt werden. Anschließend muss auf *Weiter* geklickt werden.

Unter *Bond slaves* werden die Netzwerkkarten ausgewählt, die Teil des Bonding-Interfaces sind. Für das Failover-Szenarien (s.u.) können über *Bond primary* die Netzwerkkarten ausgewählt werden, die bevorzugt verwendet werden sollen.

Der *Modus* konfiguriert die Verteilung der Netzwerkkarten innerhalb des Bondings:

- `balance-rr (0)` verteilt die Pakete der Reihe nach gleichmässig auf die verfügbaren Netzwerkschnittstellen innerhalb des Bondings. Dies erhöht den Durchsatz und verbessert die Ausfallsicherheit. Zur Verwendung dieser Variante müssen die verwendeten Netzwerk-Switches *Link Aggregation* unterstützen.
- Bei Verwendung von `active-backup (1)` ist nur jeweils eine Netzwerkkarte des Bonding-Interfaces aktiv (in der Grundeinstellung die Netzwerkschnittstelle aus *Bond primary*). Fällt die primäre Netzwerkkarte aus, wird dies durch den Linux-Kernel erkannt und auf eine der weiteren Karten des Bondings umgeschaltet. Diese Variante erhöht die Ausfallsicherheit. Sie kann mit jedem Netzwerk-Switch verwendet werden.

Darüber hinaus existieren noch weitere Bonding-Methoden. Diese sind in der Regel nur für Sonderfälle relevant und sind unter Linux Ethernet Bonding Driver HOWTO[35] beschrieben.

Zur Erkennung ausgefallener Netzwerkverbindungen wird das Media Independent Interface (MII) der Netzwerkkarten verwendet. Die Einstellung *MII link monitoring frequency* legt das Prüfintervall in Millisekunden fest.

Unter *Weitere Bonding-Optionen* können beliebige weitere Bonding-Parameter konfiguriert werden. Dies ist nur in Ausnahmefällen nötig, eine Übersicht der möglichen Einstellungen findet sich in Linux Ethernet Bonding Driver HOWTO[36].

Nach einem Klick auf *Weiter* kann dem Bonding-Interface eine IP-Adresse zugewiesen werden. Sollte eine der bestehenden Netzwerkkarten, die Bestandteil des Bonding-Interfaces sind, schon eine IP-Adresse zugewiesen haben, so wird diese Konfiguration entfernt. Die Einstellungsmöglichkeiten sind dieselben wie in *Konfiguration von IPv4-Adressen* (Seite 156) und *Konfiguration von IPv6-Adressen* (Seite 156) beschrieben.

Konfiguration VLAN

VLANs können verwendet werden um den Netzwerkverkehr in einem physischen Netzwerk logisch auf ein oder mehrere virtuelle Unternetze aufzuteilen. Jedes dieser virtuellen Netze ist eine eigenständige Broadcast-Domäne. So kann etwa in einem Firmennetzwerk das Netz für die Mitarbeiter von einem Gastnetz für Besucher unterschieden werden, obwohl die selbe physikalische Verkabelung genutzt wird. Die Zuordnung der einzelnen Endgeräte zu den VLANs erfolgt durch Konfiguration auf den verwendeten Switches. Die Netzwerk-Switches müssen 802.1q VLANs unterstützen.

Es werden zwei Typen von Verbindungen zwischen Netzwerkkarten unterschieden:

- Eine Verbindung transportiert nur Pakete eines spezifischen VLANs. In diesem Fall werden die Datenpakete ungetagged übertragen.

[35] https://www.kernel.org/doc/Documentation/networking/bonding.txt
[36] https://www.kernel.org/doc/Documentation/networking/bonding.txt

Dies ist typischerweise der Fall, wenn nur ein einzelnes Endgerät über diese Netzwerkverbindung angebunden wird.

- Eine Verbindung transportiert Pakete aus mehreren VLANs. Dies wird auch als *trunk link* bezeichnet. In diesem Fall ist jedes Paket über eine VLAN-ID einem VLAN zugeordnet. Bei der Weiterleitung zwischen *trunk links* und spezifischen VLANs übernimmt der Netzwerk-Switch die Aufgabe, anhand der VLAN-IDs die Pakete zu filtern und die VLAN-IDs hinzuzufügen und zu entfernen.

  Diese Verbindungsart wird vornehmlich zwischen Switches und Servern eingesetzt.

  Einige Switches erlauben es auch Pakete mit und ohne VLAN-Tag über eine gemeinsame Verbindung zu schicken, darauf wird hier aber nicht weiter eingegangen.

Mit der Konfiguration eines VLANs im UMC-Modul *Netzwerk-Einstellungen* kann für einen Rechner konfiguriert werden, an welchen VLANs er teilnehmen möchte. Ein Beispiel wäre ein interner Firmen-Webserver, der sowohl für die Mitarbeiter, als auch für die Benutzer des Gastnetzes verfügbar sein soll.

Um ein VLAN zu konfigurieren muss unter *Hinzufügen* als *Netzwerkgerätetyp* `Virtuelles LAN` ausgewählt werden. Die Netzwerkschnittstelle, für die das VLAN konfiguriert wird, wird mit *Übergeordnetes Netzwerkgerät* angegeben. Die *VLAN ID* ist der eindeutige Bezeichner für das VLAN. Gültige Werte sind 1 bis 4095. Anschließend muss auf *Weiter* geklickt werden.

Nach einem Klick auf *Weiter* kann dem VLAN-Interface eine IP-Adresse zugewiesen werden. Die Einstellungsmöglichkeiten sind dieselben wie in *Konfiguration von IPv4-Adressen* (Seite 156) und *Konfiguration von IPv6-Adressen* (Seite 156) beschrieben. Bei der Vergabe einer IP-Adresse muss darauf geachtet werden, dass die Adresse zum zugeordneten VLAN-Adressbereich passt.

8.2.5 Konfiguration des Proxyzugriffs

Die meisten Kommandozeilen-Tools, die Zugriffe auf Webserver durchführen (z.B. **`wget`**, **`elinks`** oder **`curl`**), prüfen, ob die Umgebungsvariablen `http_proxy` oder `https_proxy` gesetzt sind. Ist dies der Fall, werden automatisch die in diesen Variablen eingestellte Proxy-Server verwendet.

Über die Univention Configuration Registry Variablen *`proxy/http`* (Seite 316) und *`proxy/https`* (Seite 316) kann das Setzen dieser Umgebungsvariablen durch einen Eintrag in `/etc/profile` aktiviert werden.

Dabei muss die Proxy-URL angegeben werden, also z.B. `http://192.0.2.100`. In Proxy-URL kann optional auch die Angabe eines Ports folgen, welcher durch einen Doppelpunkt abzutrennen ist, z.B. `http://192.0.2.100:3128`. Erfordert der Proxy eine Authentifizierung, so können die Benutzerinformationen in der Form `http://`*`username`*`:`*`password`*`@192.0.2.100` übergeben werden.

Die Umgebungsvariable wird nicht für aktuell geöffnete Sitzungen übernommen. Damit die Änderung aktiv wird, muss eine Neuanmeldung erfolgen.

Die UCS-Programme zur Paketverwaltung unterstützen ebenfalls den Betrieb über einen Proxy und lesen die Univention Configuration Registry-Variable direkt aus.

Einzelne Domänen können von der Verwendung des Proxys ausgenommen werden, in dem sie kommasepariert in die Univention Configuration Registry Variable *`proxy/no_proxy`* (Seite 316) aufgenommen werden. Unterdomänen werden dabei berücksichtigt; eine Ausnahme für `software-univention.de` wirkt sich also auch auf `updates.software-univention.de` aus.

8.2.6 Einbinden von NFS-Freigaben

Mit der Richtlinie *NFS-Freigaben* in den UMC-Modulen für die Rechnerverwaltung können NFS-Freigaben konfiguriert werden, die auf dem System gemountet werden. Zur Auswahl steht eine *NFS-Freigabe*, die unter dem in *Mount point* angegebenen Dateipfad eingehängt wird.

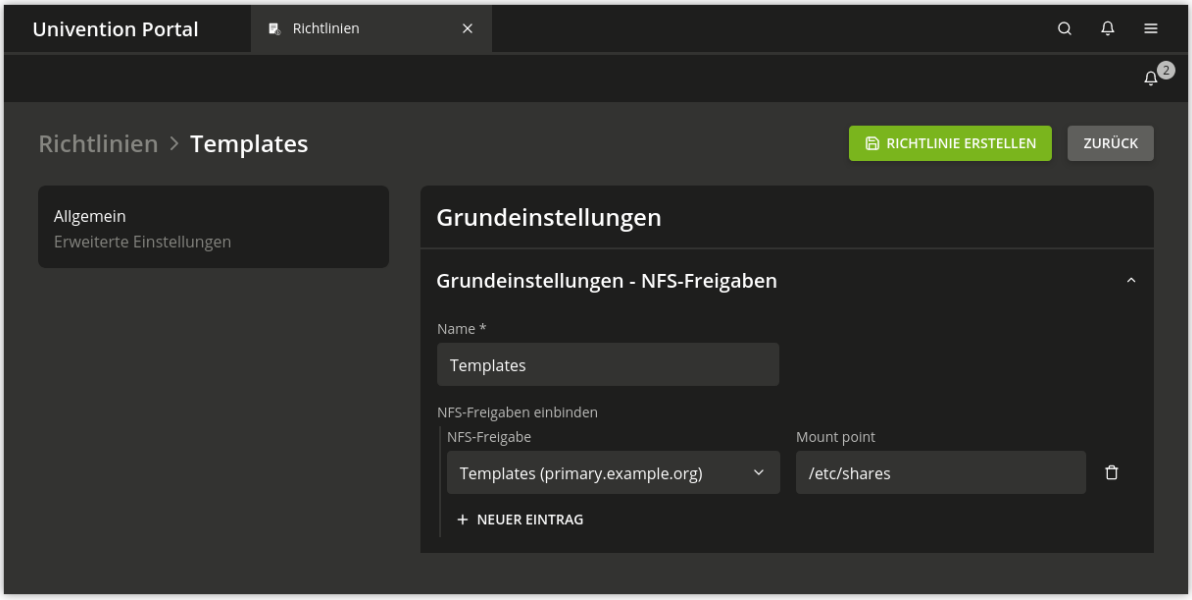


Abb. 8.5: Einbinden einer NFS-Freigabe

8.2.7 Erfassung von unterstützter Hardware

Univention erfasst Informationen über Hardware, die mit UCS kompatibel und bei Kunden im Einsatz ist. Die hierbei verarbeiteten Informationen werden über das UMC-Modul *Hardwareinformationen* erfasst.

Alle Daten werden dabei anonymisiert an Univention weitergeleitet und erst nach Benutzereinwilligung übermittelt.

Im Start-Dialog finden sich die Eingabefelder *Hersteller* und *Modell*, die mit aus den DMI-Informationen der Hardware ermittelten Werten vorausgefüllt sind. Die Felder können auch angepasst und ein zusätzlicher *Kommentar* angegeben werden.

Wenn die Übermittlung der Hardwareinformationen im Rahmen einer Support-Anfrage erfolgt, sollte die Option *Dies bezieht sich auf einen Supportfall* aktiviert werden. Im folgenden Feld kann dann eine Ticketnummer angegeben werden, die die Zuordnung vereinfacht und eine schnellere Bearbeitung ermöglicht.

Nach einem Klick auf *Weiter* wird eine Übersicht der ermittelten Hardwareinformationen ausgegeben. Außerdem wird ein komprimiertes Tar-Archiv erstellt, das eine Liste mit den im System verwendeten Hardware-Komponenten enthält und über *Archiv mit den Hardwareinformationen* heruntergeladen werden kann.

Nach einem erneuten Klick auf *Weiter* kann der Übermittlungsweg der Daten an Univention ausgewählt werden. *Hochladen* überträgt die Daten per HTTPS, *Mail senden* führt zu einem Dialog, der die für den Versand nötigen Schritte aufführt.

8.3 Verwaltung der lokalen Systemkonfiguration mit Univention Configuration Registry

Univention Configuration Registry ist das zentrale Werkzeug zur Verwaltung der lokalen Systemkonfiguration eines UCS-basierten Systems. Ein direktes Editieren der Konfigurationsdateien ist dabei in der Regel nicht nötig.

Einstellungen werden in einem Registrierungsmechanismus in einem einheitlichen Format festgelegt, den sogenannten *Univention Configuration Registry-Variablen*. Diese Variablen werden verwendet, um aus Konfigurationsdatei-Vorlagen (den sogenannten *Univention Configuration Registry-Templates*) die effektiv von den Diensten/Programmen verwendeten Konfigurationsdateien zu generieren.

Dieses Verfahren bietet eine Reihe von Vorteilen:

- In der Regel müssen keine Konfigurationsdateien manuell editiert werden. Dies vermeidet Fehler durch ungültige Syntax von Konfigurationseinstellungen o.ä.
- Es existiert ein einheitliches Interface zum Editieren der Einstellungen und die unterschiedlichen Syntaxformate der Konfigurationsdateien werden vor dem Administrator verborgen.
- Die Einstellungen werden von der eigentlichen Konfigurationsdatei entkoppelt, d.h. wenn eine Software in einer neuen Version ein anderes Konfigurationsformat verwendet, wird einfach ein neues Template im neuen Format ausgeliefert anstatt eine aufwendige und fehlerträchtige Konvertierung der bestehenden Konfigurationsdatei vorzunehmen.
- Die in einer durch Univention Configuration Registry verwalteten Konfigurationsdatei verwendeten Variablen werden intern zugeordnet. Das stellt sicher, dass beim Ändern einer UCR-Variable alle Konfigurationsdateien, auf die sich die veränderte Variable bezieht, neu erstellt werden.

Univention Configuration Registry-Variablen können auf der Kommandozeile über den Befehl **`univention-config-registry`** (Kurzform: **`ucr`**) oder über das UMC-Modul *Univention Configuration Registry* konfiguriert werden.

Da die meisten Pakete ihre Konfiguration über Univention Configuration Registry durchführen und bei der Installation entsprechende Grundeinstellungen eingerichtet werden, sind nach der Installation eines UCS-Systems bereits einige Hundert Univention Configuration Registry-Variablen gesetzt.

UCR-Variablen können auch effizient in Shell-Skripten verwendet werden, um auf Systemeinstellungen wie den Rechnernamen zuzugreifen.

Die Benennung der Variablen folgt einer baumartigen Struktur, wobei ein Schrägstrich als Trennzeichen von Namensbestandteilen verwendet wird. Beispielsweise handelt es sich bei allen mit `ldap` beginnenden Univention Configuration Registry-Variablen um Einstellungen, die den lokalen Verzeichnisdienst betreffen.

Zu den meisten Variablen ist eine Beschreibung hinterlegt, die die Verwendung und Funktion erläutert.

Wenn eine Konfigurationsdatei durch ein UCR-Template verwaltet wird und die gewünschte Einstellung nicht bereits durch eine vorhandene Variable abgedeckt ist, muss statt der Konfigurationsdatei das UCR-Template erweitert werden. Würde die Konfigurationsdatei direkt angepasst, würde bei der nächsten Neugenerierung der Datei - z.B. beim Setzen einer registrierten UCR-Variable - die lokale Anpassung wieder überschrieben. Die Anpassung von UCR-Templates ist in *Anpassung von UCR-Templates* (Seite 165) beschrieben.

Ein Teil der über Univention Configuration Registry konfigurierten Einstellungen sind systemspezifisch (z.B. der Rechnername), viele Eigenschaften können jedoch auch auf mehrere Rechner angewendet werden. Mithilfe der *Univention Configuration Registry-Richtlinie* in den UMC-Modulen zur Domänenverwaltung können Variablen zusammengefasst und auf mehr als einen Rechner angewendet werden.

Die Auswertung der Univention Configuration Registry-Variablen auf einem UCS-System erfolgt vierstufig:

- Als Erstes werden lokale Univention Configuration Registry-Variablen ausgewertet.
- Die lokalen Variablen werden von Richtlinien-Variablen überstimmt, die aus dem Verzeichnisdienst bezogen werden

- Die Option `--schedule` dient zum Setzen lokaler Variablen, die nur für einen gewissen Zeitraum gelten sollen. Diese Ebene der Univention Configuration Registry ist reserviert für lokale Einstellungen, die durch zeitgesteuerte Mechanismen in Univention Corporate Server automatisiert vorgenommen werden.
- Durch Verwendung der Option `--force` beim Setzen einer lokalen Variable werden aus den Verzeichnisdienst übernommene Einstellung ebenso wie Variablen der Schedule-Ebene überstimmt und statt dessen der angegebene Wert für das lokale System festgelegt. Beispiel:

```
$ univention-config-registry set --force mail/messagesizelimit=1000000
```

Wird eine Variable gesetzt, die durch eine übergeordnete Richtlinie überschrieben wird, erscheint eine Warnmeldung.

Die Verwendung der Univention Configuration Registry-Richtlinie ist in *Richtlinienbasierte Konfiguration von UCR-Variablen* (Seite 164) dokumentiert.

8.3.1 Verwendung des Univention Management Console Moduls

Über das UMC-Modul *Univention Configuration Registry* können die Variablen eines Systems angezeigt und verändert werden, außerdem besteht die Möglichkeit über *Hinzufügen* neue Variablen zu setzen.

Auf der Startseite wird eine Suchmaske angezeigt. Alle Variablen sind anhand einer *Kategorie* klassifiziert, etwa alle LDAP-bezogenen Einstellungen.

In der Suchmaske kann als Filter das *Suchattribut* angegeben werden, das sich auf den Variablennamen, den Wert oder die Beschreibung beziehen kann.

Nach erfolgter Suche werden die gefundenen Variablen in einer Tabelle angezeigt, dabei wird der Variablenname und der Wert angezeigt. Bewegt man den Mauszeiger auf den Variablennamen, wird eine weiterführende Beschreibung der Variable angezeigt.

Eine Variable kann mit einem Klick auf ihren Namen bearbeitet werden. Mit einem Rechts-Klick und der Auswahl von *Löschen* können Variablen gelöscht werden.

8.3.2 Verwendung des Kommandozeilenfrontends

Das Kommandozeileninterface von Univention Configuration Registry wird über den Befehl **`univention-config-registry`** aufgerufen. Alternativ kann auch die Kurzform **`ucr`** verwendet werden.

Abfrage einer UCR-Variable

`get`

Eine einzelne Univention Configuration Registry-Variable kann mit dem Aufrufparameter *`get`* (Seite 162) ausgelesen werden:

```
$ univention-config-registry get ldap/server/ip
```

`dump`

Mit dem Aufrufparameter *`dump`* (Seite 162) können auch alle aktuell gesetzten Variablen ausgegeben werden:

```
$ univention-config-registry dump
```

Setzen von UCR-Variablen

set

Mit dem Aufrufparameter *set* (Seite 163) kann eine Variable gesetzt werden. Der Name der Variable kann frei gewählt werden, darf aber ausschließlich aus Buchstaben, Punkten, Zahlen, Binde- und Schrägstrichen bestehen.

```
$ univention-config-registry set VARIABLENNAME=WERT
```

Ist die Variable schon vorhanden, wird der Inhalt aktualisiert. Ansonsten wird ein neuer Eintrag angelegt.

Beim Setzen eines neuen Wertes für eine Univention Configuration Registry-Variable führt UCR Prüfungen durch, um die Kompatibilität des Wertes mit dem Variablentyp zu überprüfen. Im Falle einer Inkompatibilität zeigt UCR eine Warnmeldung an. Außerdem wird die Variable nicht auf den neuen Wert gesetzt, wenn die Univention Configuration Registry-Variable *ucr/check/type* (Seite 319) auf `true` steht (Standard ist `false`). Wenn die Option `--ignore-check` verwendet wird, wird der Wert immer gesetzt, unabhängig von der Typ-Kompatibilität und der Einstellung von *ucr/check/type* (Seite 319).

Wenn sich eine Variable ändert, schreibt UCR sofort alle Konfigurationsdateien neu, für die die Variable registriert ist. UCR gibt die Pfade der aktualisierten Dateien auf der Konsole aus.

Dabei ist zu beachten, dass beim Setzen einer UCR-Variable zwar die Konfiguration eines Dienstes aktualisiert wird, der entsprechende Dienst aber nicht automatisch neu gestartet wird! Der Neustart muss manuell erfolgen.

Gleichzeitige Änderungen mehrerer Variablen in einer Befehlszeile sind möglich. Wenn sich diese auf ein- und dieselbe Konfigurationsdatei beziehen, wird diese nur einmal neu geschrieben.

```
$ univention-config-registry set \
  dns/forwarder1=192.0.2.2 \
  sshd/xforwarding="no" \
  sshd/port=2222
```

Auch ein bedingtes Setzen ist möglich. Soll z.B. ein Wert nur dann in einer Univention Configuration Registry-Variable gespeichert werden, wenn die Variable noch nicht vorhanden ist, kann dies durch ein Fragezeichen (`?`) statt des Gleichheitszeichens (`=`) beim Zuweisen des Wertes erreicht werden.

```
$ univention-config-registry set dns/forwarder1?192.0.2.2
```

Suche nach Variablen und gesetzten Werten

search

Mit dem Parameter *search* (Seite 163) kann nach einer Variable gesucht werden. Dieser Befehl sucht nach Variablennamen, welche die Zeichenkette `nscd` enthalten und gibt diese mit den aktuellen Belegungen aus:

```
$ univention-config-registry search nscd
```

Es kann alternativ auch nach gesetzten Variablen-Werten gesucht werden. Dieser Aufruf sucht nach allen Variablen, die auf `primary.example.com` gesetzt sind:

```
$ univention-config-registry search --value primary.example.com
```

Bei der Suche können auch Suchmuster in Form von regulären Ausdrücken verwendet werden. Das vollständige Format ist unter Regular expression operations in the Python 3 documentation[37] dokumentiert.

[37] https://docs.python.org/3/library/re.html

Löschen von UCR-Variablen

unset

Mit dem Aufrufparameter *unset* (Seite 164) kann eine Variable entfernt werden. Das folgende Beispiel löscht die Variable *dns/forwarder2* (Seite 305). Auch hier können mehrere zu löschende Variablen übergeben werden:

```
$ univention-config-registry unset dns/forwarder2
```

Neuerzeugung von Konfigurationsdateien aus ihrem Template

commit

Mit dem Aufrufparameter *commit* (Seite 164) wird eine Konfigurationsdatei aus ihrem Template neu erzeugt. Der Name der Konfigurationsdatei ist als Parameter anzugeben, z.B.:

```
$ univention-config-registry commit /etc/samba/smb.conf
```

Da UCR-Templates beim Editieren von UCR-Variablen in der Regel automatisch neu erzeugt werden, wird dies vor allem für Tests verwendet.

Wird beim Aufruf von **ucr commit** kein Dateiname angegeben, werden sämtliche durch Univention Configuration Registry verwalteten Dateien neu aus den Vorlagen erzeugt. In der Regel sollte es allerdings nicht notwendig sein, alle Konfigurationsdateien neu zu erzeugen.

Übernahme von Variablen in Shell-Skripte

shell

Über den Aufrufparameter *shell* (Seite 164) werden Univention Configuration Registry-Variablen und ihre aktuellen Belegungen in einem Format ausgegeben, das in Shell-Skripten verwendet werden kann.

```
$ univention-config-registry shell ldap/server/name
```

Dabei werden verschiedene Konvertierungen vorgenommen: Schrägstriche in Variablennamen werden durch Unterstriche ersetzt und in den Werten enthaltene Zeichen, die in Shell-Skripten eine besondere Bedeutung haben, werden durch Anführungszeichen geschützt.

Damit Univention Configuration Registry-Variablen als Umgebungsvariablen in einem Shell-Skript eingelesen werden, muss die Ausgabe von Univention Configuration Registry durch den Befehl **eval** ausgeführt werden:

```
# eval "$(univention-config-registry shell ldap/server/name)"
# echo "$ldap_server_name"
primary.firma.de
```

8.3.3 Richtlinienbasierte Konfiguration von UCR-Variablen

Ein Teil der über Univention Configuration Registry konfigurierten Einstellungen sind systemspezifisch (z.B. der Rechnername), viele Eigenschaften können jedoch auch auf mehrere Rechner angewendet werden. Mithilfe der im UMC-Modul *Richtlinien* verwalteten *Univention Configuration Registry*-Richtlinie können Variablen zusammengefasst und auf mehr als einen Rechner angewendet werden.

Zuerst muss für die anzulegende Richtlinie ein *Name* gesetzt werden, unter dem die Variablen später einzelnen Rechner-Objekten zugewiesen werden können.

Außerdem muss mindestens eine *Variable* konfiguriert und ein *Wert* zugewiesen werden.

Diese Richtlinie kann dann einem Rechner-Objekt oder einem Container/OU zugewiesen werden (siehe *Zuweisung von Richtlinien* (Seite 78)). Es ist zu beachten, dass die Auswertung der konfigurierten Werte gegenüber den übrigen Richtlinien abweicht: Die Werte werden nicht direkt auf die Rechner übertragen, sondern durch Univention

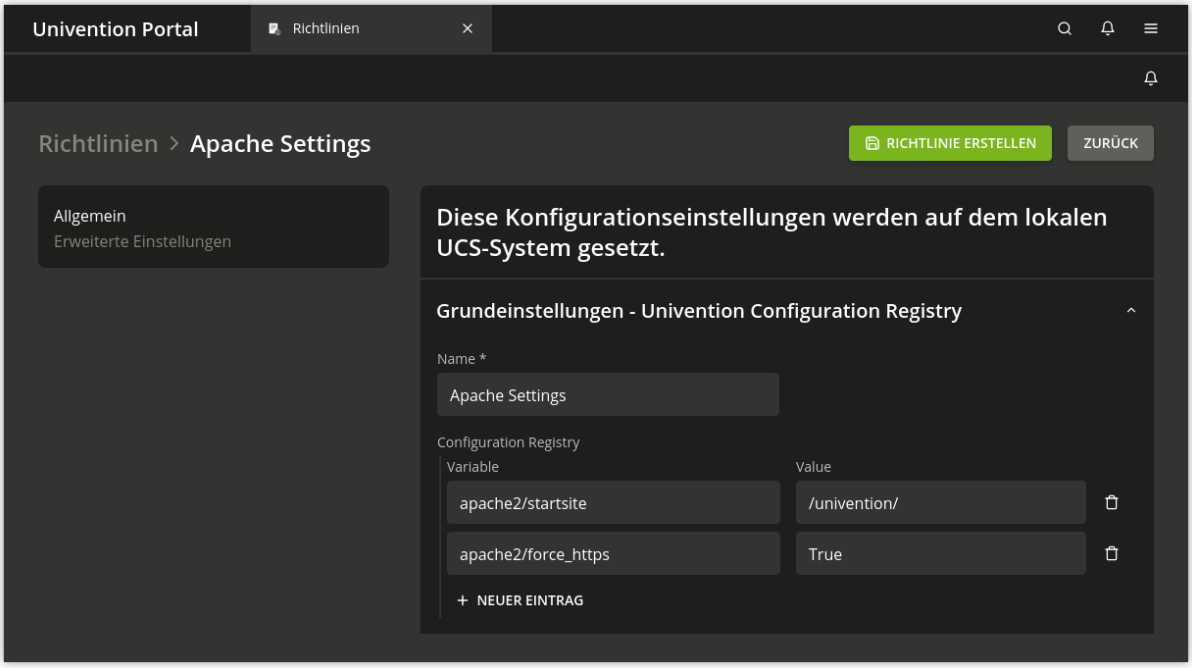


Abb. 8.6: Richtlinienbasierte Konfiguration der Webserver Startseite mit forciertem HTTPS

Directory Policy auf den zugewiesenen Rechner geschrieben. Das dabei verwendete Zeitintervall wird durch die Univention Configuration Registry Variable *ldap/policy/cron* (Seite 309) konfiguriert und erfolgt standardmäßig stündlich.

8.3.4 Anpassung von UCR-Templates

Ein Univention Configuration Registry-Template ist im einfachsten Fall eine Kopie der ursprünglichen Konfigurationsdatei, in der die Stellen, an denen der Wert einer Variable verwendet werden soll, eine Referenz auf den Variablennamen enthalten.

Für komplexere Szenarien kann auch Inline-Python-Code integriert werden, der dann auch komplexere Konstrukte wie etwa bedingte Abfragen erlaubt.

Bemerkung: Univention Configuration Registry-Templates sind in den entsprechenden UCS-Software-Paketen als Konfigurationsdateien enthalten. Bei der Aktualisierung von Paketen wird überprüft, ob Änderungen an Konfigurationsdateien vorgenommen wurden.

Wenn Konfigurationsdateien nicht mehr im Auslieferungszustand vorliegen, werden diese nicht überschrieben. Stattdessen wird eine neue Version im selben Verzeichnis mit der Endung `.debian.dpkg-new` abgelegt.

Sollen Änderungen an Univention Configuration Registry-Templates vorgenommen werden, werden diese Templates bei der Aktualisierung ebenfalls nicht überschrieben und im selben Verzeichnis mit der Endung `.dpkg-new` oder `.dpkg-dist` abgelegt. Entsprechenden Hinweise werden in die Log-Datei `/var/log/univention/updater.log` geschrieben. Dies tritt nur auf, wenn UCR-Templates lokal angepasst werden.

Die UCR-Templates werden im Verzeichnis `/etc/univention/templates/files/` abgelegt. Der Pfad zu den Vorlagen entspricht dem absoluten Pfad zu der Konfigurationsdatei mit vorangestelltem Pfad zum Vorlagenverzeichnis. So findet sich zum Beispiel die Vorlage für die Konfigurationsdatei `/etc/issue` unter `/etc/univention/templates/files/etc/issue`.

Damit Konfigurationsdateien von Univention Configuration Registry korrekt verarbeitet werden können, müssen sie im UNIX-Format vorliegen. Werden Konfigurationsdateien z.B. unter DOS oder Windows bearbeitet, werden Steu-

erzeichen zur Kennzeichnung des Zeilenumbruchs eingefügt, die die Verwendung der Datei durch Univention Configuration Registry stören.

Referenzierung von UCR-Variablen in Templates

Im einfachsten Fall kann eine UCR-Variable im Template direkt referenziert werden. Als Platzhalter dient der Variablenname, der von der Zeichenkette `@%@` eingefasst wird. Als Beispiel die Option für die Aktivierung von X11-Forwarding in der Konfigurationsdatei `/etc/ssh/sshd_config` des OpenSSH-Servers:

```
X11Forwarding @%@sshd/xforwarding@%@
```

Neu eingefügte Referenzen auf UCR-Variablen werden automatisch von Templates ausgewertet, eine zusätzliche Registrierung ist nur bei der Verwendung von Inline-Python-Code nötig (siehe *Integration von Inline-Python-Code in Templates* (Seite 166)).

Integration von Inline-Python-Code in Templates

In UCR-Templates kann beliebiger Python-Code eingebettet werden, in dem ein von der Zeichenkette `@!@` eingefasster Codeblock eingefügt wird. Mit solchen Blöcken können z.B. bedingte Abfragen umgesetzt werden, so dass beim Ändern eines Parameters über eine Variable weitere abhängige Einstellungen automatisch in die Konfigurationsdatei aufgenommen werden. Folgende Code-Sequenz konfiguriert beispielsweise Netzwerk-Einstellungen anhand der Univention Configuration Registry-Einstellungen:

```
@!@
if configRegistry.get('apache2/ssl/certificate'):
    print('SSLCertificateFile %s' %
        configRegistry['apache2/ssl/certificate'])
@!@
```

Alle mit der `print`-Funktion ausgegebenen Daten werden dabei in die generierte Konfigurationsdatei geschrieben. Die in Univention Configuration Registry gespeicherten Daten können über das `ConfigRegistry`-Objekt abgefragt werden, z.B.:

```
@!@
if configRegistry.get('version/version') and \
        configRegistry.get('version/patchlevel'):
    print('UCS %(version/version)s-%(version/patchlevel)s' %
        configRegistry)
@!@
```

Im Gegensatz zu direkt referenzierten UCR-Variablen (siehe *Referenzierung von UCR-Variablen in Templates* (Seite 166)) müssen Variablen, auf die in Inline-Python-Code zugegriffen wird, explizit registriert werden.

Die in Konfigurationsdateien verwendeten Univention Configuration Registry-Variablen werden unterhalb des Verzeichnisses `/etc/univention/templates/info/` in *info*-Dateien registriert, die in der Regel nach dem Paketnamen mit der Dateiendung `.info` benannt werden. Wird neuer Python-Code in die Vorlagen eingefügt oder bestehender Code so verändert, dass er zusätzliche oder andere Variablen nutzt, so muss einer der bestehenden `.info`-Dateien modifiziert oder eine neue hinzugefügt werden.

Nach der Änderung von `.info`-Dateien muss der Befehl **`ucr update`** aufgerufen werden.

8.4 Basis-Systemdienste

Dieser Abschnitt beschreibt grundlegende System-Dienste einer UCS-Installation, wie etwa die Konfiguration der Authentifizierungsschnittstelle PAM, des System-Loggings und des NSCD.

8.4.1 Administrativer Zugriff mit dem Root-Konto

Für den administrativen Vollzugriff existiert auf jedem UCS-System das `root`-Konto. Das Passwort wird beim Installieren des Systems festgelegt. Der root-Benutzer wird nicht im LDAP-Verzeichnis gespeichert, sondern in den lokalen Benutzerkonten.

Das Passwort für den lokalen root-Nutzer kann über die Kommandozeile mit dem Befehl **`passwd`** geändert werden. Es ist zu beachten, dass hierbei keine Prüfungen hinsichtlich der Passwortlänge/-Stärke und bereits verwendeter Passwörter durchgeführt wird.

8.4.2 Konfiguration der Sprach- und Tastatureinstellungen

Unter Linux werden Lokalisierungseigenschaften für Software in sogenannten *Locales* definiert. Konfiguriert werden u.a. Einstellungen wie Datums- sowie zu nutzende Währungsformate, verwendete Zeichensätze und die Sprachauswahl für internationalisierte Programme. Die installierten *Locales* können im UMC-Modul *Sprach-Einstellungen* unter *Spracheinstellungen* ‣ *Verfügbare Systemsprache* geändert werden. Unter *Standard-System-Sprachdefinition* wird die Standard-Locale festgelegt.

Das *Tastaturlayout* im Menüpunkt *Zeitzonen- und Tastatureinstellungen* greift bei lokalen Anmeldungen an dem Rechner.

8.4.3 Starten/Stoppen von Systemdiensten / Konfiguration des automatischen Starts

Mit dem UMC-Modul *Systemdienste* kann der aktuelle Status eines Systemdienstes geprüft und dieser gegebenenfalls gestartet oder gestoppt werden.

In der Liste aller auf dem System installierten Dienste ist unter *Status* der aktuelle Laufzeitstatus und eine *Beschreibung* aufgeführt. Unter *mehr* kann der Dienst gestartet, gestoppt oder neu gestartet werden.

In der Grundeinstellung wird jeder Dienst automatisch beim Systemstart gestartet. In einigen Fällen kann es sinnvoll sein, den Dienst nicht direkt zu starten, sondern z.B. erst nach Konfiguration weiterer Einstellungen. Mit der Aktion *Manuell starten* wird der Dienst nicht beim Systemstart automatisch gestartet, kann aber nachträglich gestartet werden. Mit der Aktion *Niemals starten* wird auch der nachträgliche Start unterbunden.

8.4.4 Authentifizierung / PAM

Authentifizierungsdienste werden in Univention Corporate Server durch *Pluggable Authentication Modules* (PAM) realisiert. Dabei werden unterschiedliche Anmeldeverfahren auf eine gemeinsame Schnittstelle abgebildet, so dass eine neue Anmeldemethode keine Anpassungen an bestehenden Applikationen benötigt.

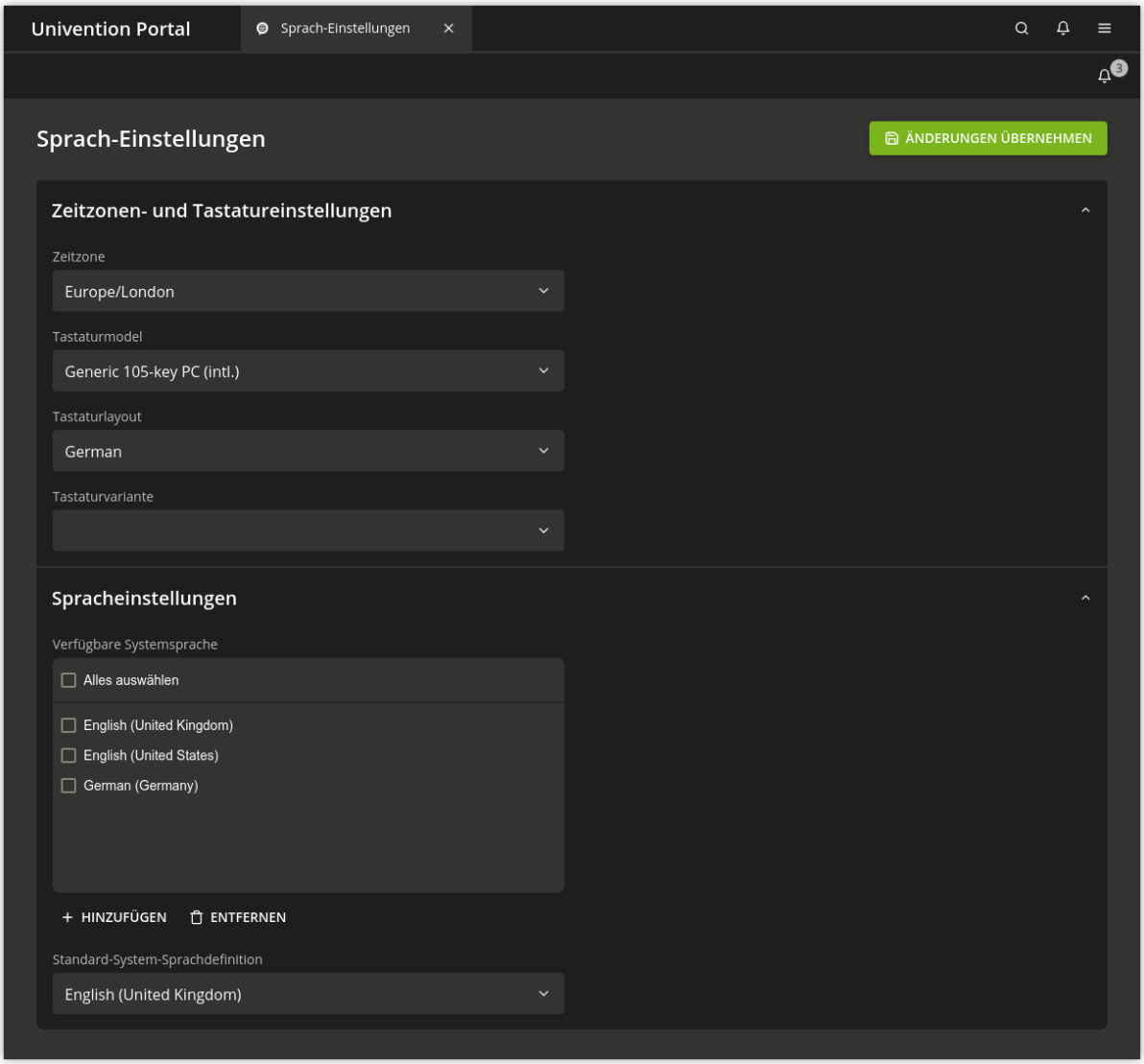


Abb. 8.7: Konfiguration der Spracheinstellungen

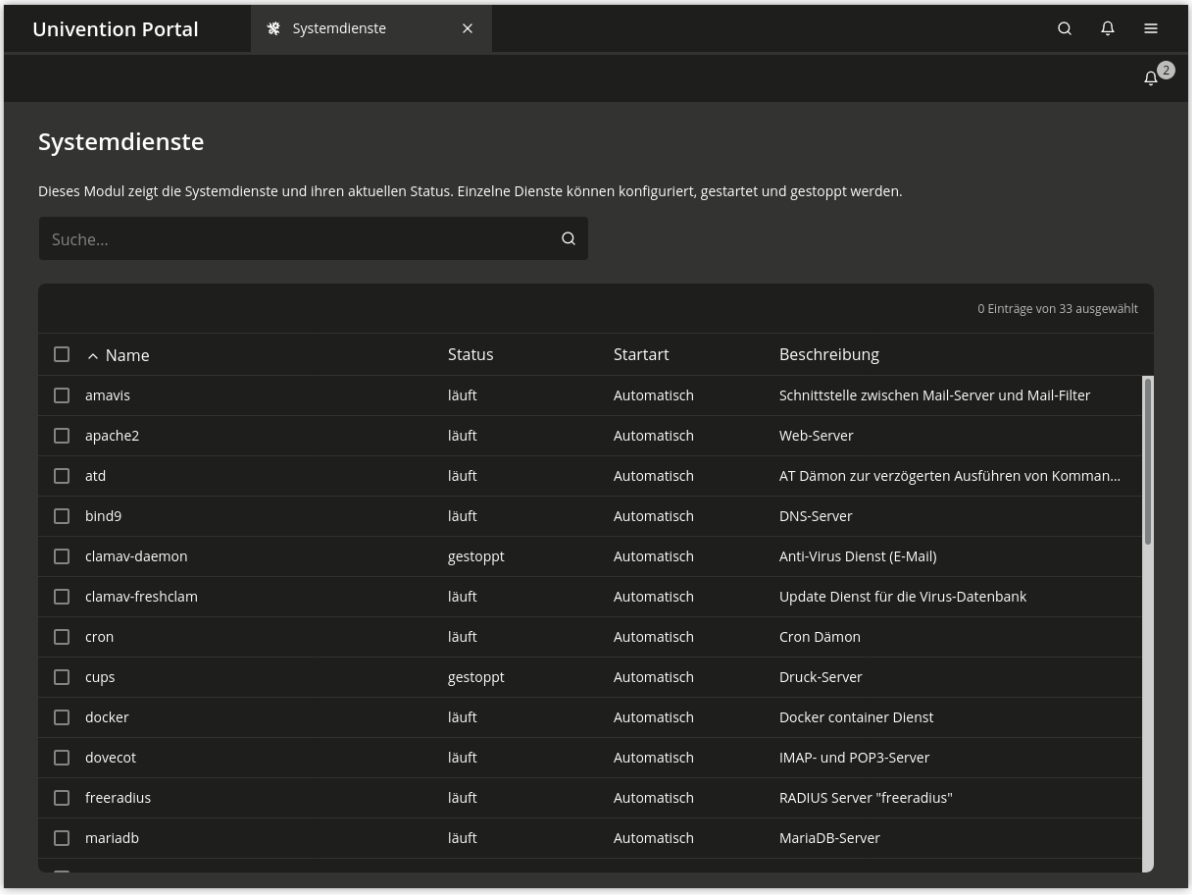


Abb. 8.8: Übersicht der Systemdienste

Anmeldebeschränkungen für ausgewählte Benutzer

In der Grundeinstellung können sich nur der `root`-Benutzer und Mitglieder der Gruppe `Domain Admins` remote über SSH und lokal auf einem `tty` anmelden.

Diese Einschränkung kann mit der Univention Configuration Registry Variable `auth/`*`DIENST`*`/restrict` konfiguriert werden. Der Zugriff auf diesen Dienst kann durch Setzen der Variablen `auth/`*`DIENST`*`/user/`*`BENUTZERNAME`* und `auth/`*`DIENST`*`/group/`*`GRUPPENNAME`* auf `yes` freigegeben werden.

Anmeldebeschränkungen werden unterstützt für *SSH* (`sshd`), Anmeldung an einem *tty* (`login`), *rlogin* (`rlogin`), *PPP* (`ppp`) und andere Dienste (`other`). Ein Beispiel für *SSH*:

```
auth/sshd/group/Administrators: yes
auth/sshd/group/Computers: yes
auth/sshd/group/DC Backup Hosts: yes
auth/sshd/group/DC Slave Hosts: yes
auth/sshd/group/Domain Admins: yes
auth/sshd/restrict: yes
```

8.4.5 Konfiguration des verwendeten LDAP-Servers

In einer UCS-Domäne können mehrere LDAP-Server betrieben werden. Der primär verwendete wird mit der Univention Configuration Registry Variable *ldap/server/name* (Seite 309) festgelegt, weitere Server können über die Univention Configuration Registry Variable *ldap/server/addition* (Seite 309) angegeben werden.

Alternativ können die LDAP-Server auch über die Richtlinie *LDAP-Server* festgelegt werden. Die Reihenfolge der Server bestimmt die Reihenfolge der Anfragen des Rechners an die Server, falls ein LDAP-Server nicht erreichbar sein sollte.

In der Grundeinstellung ist nach Installation/Domänenbeitritt nur *ldap/server/name* (Seite 309) gesetzt. Ist mehr als ein LDAP-Server vorhanden, ist es empfehlenswert zur Verbesserung der Ausfallsicherung mindestens zwei LDAP-Server über die *LDAP-Server*-Richtlinie zuzuweisen. Bei einer auf mehrere Standorte verteilten Umgebung sollte darauf geachtet werden, möglichst LDAP-Server aus dem lokalen Netz vorzugeben.

8.4.6 Konfiguration des verwendeten Druckservers

Der zu verwendende Druckserver kann mit der Univention Configuration Registry Variable *cups/server* (Seite 304) festgelegt werden.

Alternativ kann der Server auch über die Richtlinie *Druckserver* im UMC-Modul *Rechner* festgelegt werden.

8.4.7 Protokollierung/Abfrage von Systemmeldungen und -zuständen

Logdateien

Alle UCS-spezifischen Logdateien (z.B. für die Listener/Notifier-Replikation) werden im Verzeichnis `/var/log/univention/` abgelegt. Serverdienste protokollieren in ihre jeweilige Standard-Logdateien; Apache beispielsweise in die Datei `/var/log/apache2/error.log`.

Die Logdateien werden durch **`logrotate`** verwaltet. Es sorgt dafür, dass Logdateien in einem Intervall (konfigurierbar in Wochen über die Univention Configuration Registry Variable *log/rotate/weeks* (Seite 310), standardmäßig 12) fortlaufend benannt werden und ältere Logdateien anschließend gelöscht werden. Die aktuelle Logdatei für den Univention Directory Listener findet sich beispielsweise in der Datei `listener.log`, die der Vorwoche in `listener.log.1` und so weiter.

Alternativ können Logdateien auch erst beim Erreichen einer bestimmten Größe rotiert werden. Soll beispielsweise erst ab einer Größe von 50 MB rotiert werden, kann dazu die Univention Configuration Registry Variable *logrotate/rotates* (Seite 310) auf `size 50M` gesetzt werden.

Über die Univention Configuration Registry Variable *logrotate/compress* (Seite 310) kann konfiguriert werden, ob die älteren Logdateien zusätzlich mit **gzip** komprimiert werden sollen.

Logdateien, welche im Pfad `/var/log/univention/listener_modules` liegen, verfügen jeweils über eine eigene Konfiguration für **Logrotate**. Diese Logdateien haben globale und spezifische Einstellungen für **Logrotate**. Die Univention Configuration Registry Variable `logrotate/listener-modules/<directive>` konfiguriert die globalen Einstellungen. Die *logrotate(8)* Dokumentation beschreibt die Funktionalität im Detail. UCS unterstützt folgende Direktiven:

logrotate/listener-modules/rotate

Standardwert: `weekly`

logrotate/listener-modules/rotate/count

Standardwert: `12`

logrotate/listener-modules/create

Standardwert: `640 listener adm`

logrotate/listener-modules/missingok

Standardwert: `missingok`

logrotate/listener-modules/compress

Standardwert: `compress`

logrotate/listener-modules/notifempty

Standardwert: `notifempty`

Wenn eine Konfiguration nur für eine spezifische Logdatei gelten soll, muss die Univention Configuration Registry Variable wie folgt zusammengesetzt werden: `logrotate/listener-modules/<logfile-name>/<directive>`. Geben Sie den Dateinamen für `logfile-name` ohne die Dateiendung `.log` an.

Protokollierung des Systemzustands

Mit **univention-system-stats** kann der aktuelle Systemzustand in die Datei `/var/log/univention/system-stats.log` protokolliert werden. Protokolliert werden dabei folgende Werte:

- Der freie Speicherplatz auf den Systempartitionen (**df -lhT**)
- Die aktuelle Prozessliste (**ps auxf**)
- Zwei **top**-Aufstellungen der aktuellen Prozesse und Auslastung (**top -b -n2**)
- Den aktuell freien Arbeitsspeicher (**free**)
- Die Zeit, die seit dem Start des Systems vergangen ist (**uptime**)
- Temperatur-, Lüfter- und Spannungskennzahlen aus **lm-sensors** (**sensors**)
- Eine Aufstellung der aktuellen Samba-Verbindungen (**smbstatus**)

Die Laufzeiten in denen der Systemzustand protokolliert werden soll, können durch die Univention Configuration Registry Variable *system/stats/cron* (Seite 319) in Cron-Syntax definiert werden, z.B. `0,30 * * * *` für eine Protokollierung jeweils zu jeder vollen und halben Stunde. Die Protokollierung wird durch Setzen der Univention Configuration Registry Variable *system/stats* (Seite 319) auf `yes` aktiviert und ist bei Neuinstallationen ab UCS 3.0 die Grundeinstellung.

Prozessübersicht über Univention Management Console Modul

Das UMC-Modul *Prozessübersicht* zeigt eine Tabelle der aktuellen Prozesse auf dem System an. Die Prozesse können nach den folgenden Eigenschaften sortiert werden, in dem auf den entsprechenden Tabellenkopf geklickt wird:

- Die CPU-Nutzung in Prozent
- Der Benutzername, unter dem der Prozess läuft
- Speicherverbrauch in Prozent
- Die Prozess-ID

Unter dem Menüpunkt *mehr* können Prozesse beendet werden. Hierbei werden zwei Arten der Terminierung unterschieden:

Beenden
: Die Aktion *Beenden* schickt dem Prozess eine Benachrichtigung vom Typ `SIGTERM`, dies ist der Regelfall bei der kontrollierten Beendigung von Programmen.

Beenden erzwingen
: In Einzelfällen kann es vorkommen, dass sich ein Programm - z.B. nach einem Absturz - nicht mehr über dieses Verfahren beenden lässt. In diesem Fall kann mit der Aktion *Beenden erzwingen* das Signal `SIGKILL` geschickt werden, um den Prozess forciert zu beenden.

Das Beenden über `SIGTERM` ist in der Regel vorzuziehen, da viele Programme dann einen kontrollierten Programmabbruch einleiten und z.B. ein Speichern von Dateien o.ä. durchführen.

Systemdiagnose über Univention Management Console Modul

Um ein UCS-System auf verschiedene bekannte Probleme hin zu analysieren bietet das UMC-Modul *Systemdiagnose* eine entsprechende Benutzerschnittstelle.

Das Modul wertet eine Reihe ihm bekannter Problemszenarien aus und bietet Lösungsvorschläge an, wenn es in der Lage ist, gefundene Probleme automatisch zu beheben. Diese Funktion wird durch zusätzliche Schaltflächen dargestellt. Darüber hinaus werden Links zu weiterführenden Artikeln und zu entsprechenden UMC-Modulen angezeigt.

8.4.8 Ausführen von wiederkehrenden Aktionen mit Cron

Regelmäßig wiederkehrende Aktionen (wie z.B. das Verarbeiten von Logdateien) können mit dem Cron-Dienst zu einem definierten Zeitpunkt gestartet werden. Eine solche Aktion bezeichnet man auch als Cron-Job.

Stündliches/tägliches/wöchentliches/monatliches Ausführen von Skripten

Auf jedem UCS-System sind vier Verzeichnisse vordefiniert, `/etc/cron.hourly/`, `/etc/cron.daily/`, `/etc/cron.weekly/` und `/etc/cron.monthly/`. Shell-Skripte, die in diesen Verzeichnissen abgelegt werden und als ausführbar markiert sind, werden automatisch stündlich, täglich, wöchentlich oder monatlich ausgeführt.

Definition eigener Cron-Jobs in `/etc/cron.d/`

Ein Cron-Job wird in einer Zeile definiert, die aus insgesamt sieben Spalten aufgebaut ist:

- Minute (0-59)
- Stunde (0-23)
- Tag (1-31)
- Monat (1-12)
- Wochentag (0-7) (0 und 7 stehen beide für Sonntag)

- Name des ausführenden Benutzers (z.B. `root`)
- Der auszuführende Befehl

Die Zeitangaben können dabei in verschiedenen Formaten vorgenommen werden. Es kann entweder eine konkrete Minute oder Stunde vorgegeben werden oder mit einem `*` eine Aktion zu jeder Minute oder Stunde ausgeführt werden. Es können auch Intervalle definiert werden, `*/2` führt als Minutenangabe beispielsweise dazu, dass eine Aktion jede zweite Minute ausgeführt wird.

Beispiel:

```
30 * * * * root /usr/sbin/jitter 600 /usr/share/univention-samba/slave-sync
```

Definition eigener Cron-Jobs in Univention Configuration Registry

Cron-Jobs können auch in Univention Configuration Registry definiert werden. Das ist besonders nützlich, wenn sie über eine Univention Directory Manager-Richtlinie gesetzt und somit auf mehr als einen Rechner angewendet werden.

Jeder Cron-Job setzt sich dabei aus mindestens zwei Univention Configuration Registry-Variablen zusammen. `JOBNAME` ist dabei ein allgemeiner Bezeichner.

- `cron/`*`JOBNAME`*`/command` legt den auszuführenden Befehl fest (Angabe erforderlich)
- `cron/`*`JOBNAME`*`/time` setzt die Ausführungszeit fest (siehe *Definition eigener Cron-Jobs in /etc/cron.d/* (Seite 172)) (Angabe erforderlich)
- Standardmäßig wird der Cron-Job als Benutzer `root` ausgeführt. Mit `cron/`*`JOBNAME`*`/user` kann ein abweichender Benutzer angegeben werden.
- Wird unter `cron/`*`JOBNAME`*`/mailto` eine E-Mail-Adresse hinterlegt, wird die Ausgabe des Cron-Jobs per E-Mail dorthin gesendet.
- Mit `cron/`*`JOBNAME`*`/description` kann eine Beschreibung hinterlegt werden.

8.4.9 Name Service Cache Daemon

Um häufige Anfragen unveränderter Daten zu beschleunigen, werden Namensauflösungen durch den *Name Service Cache Daemon* (NSCD) zwischengespeichert. Werden diese erneut angefragt, muss so nicht eine vollständige neue LDAP-Anfrage durchgeführt werden, sondern die Daten können direkt aus dem Cache bezogen werden.

Die Zwischenspeicherung der Gruppen erfolgt seit UCS 3.1 aus Performance- und Stabilitätsgründen nicht mehr über den NSCD, sondern durch einen lokalen Gruppencache, siehe *Lokaler Gruppencache* (Seite 143).

Die zentrale Konfigurations-Datei des NSCD (`/etc/nscd.conf`) wird durch Univention Configuration Registry verwaltet.

Der Zugriff auf den Cache erfolgt über eine Hash-Tabelle. Die Größe dieser Hash-Tabelle kann über Univention Configuration Registry konfiguriert werden und sollte größer sein als die Anzahl der gleichzeitig verwendeten Benutzer/Rechner. Aus technischen Gründen sollte als Größe der Tabelle eine Primzahl verwendet werden. Die folgende Tabelle führt die Standardwerte der Variablen auf:

Tab. 8.8: Standardgröße der Hash-Tabelle

Variable	Standardgröße der Hash-Tabelle
`nscd/hosts/size`	`6007`
`nscd/passwd/size`	`6007`

Bei sehr großen Caches kann es nötig sein, die Größe der Cache-Datenbank im Arbeitsspeicher zu erhöhen. Dies kann mit den Univention Configuration Registry-Variablen *`nscd/hosts/maxdbsize`* (Seite 313), *`nscd/group/maxdbsize`* (Seite 313) und *`nscd/passwd/maxdbsize`* (Seite 313) konfiguriert werden.

Standardmäßig startet NSCD fünf Threads. In Umgebungen, in denen viele Zugriffe erfolgen, kann es erforderlich sein, die Anzahl durch die Univention Configuration Registry Variable *nscd/threads* (Seite 313) zu erhöhen.

In der Grundeinstellung wird ein aufgelöster Gruppen- oder Rechnername eine Stunde im Cache vorgehalten und ein Benutzername zehn Minuten. Durch die Univention Configuration Registry-Variablen *nscd/group/positive_time_to_live* (Seite 313), *nscd/hosts/positive_time_to_live* (Seite 313) und *nscd/passwd/positive_time_to_live* (Seite 313) können diese Zeiträume erweitert oder verringert werden (die Angabe erfolgt in Sekunden).

Gelegentlich kann es nötig sein, den Cache des NSCD manuell zu invalidieren. Dies kann individuell pro Cache-Tabelle durch folgende Befehle geschehen:

```
$ nscd -i passwd
$ nscd -i hosts
```

Der Detailgrad der Logmeldungen kann mit der Univention Configuration Registry Variable *nscd/debug/level* (Seite 313) konfiguriert werden.

8.4.10 SSH-Zugriff auf Systeme

Bei der Installation eines UCS-Systems wird in der Vorauswahl ein SSH-Server mitinstalliert. Über SSH können verschlüsselte Verbindungen zu Rechnern aufgebaut werden, wobei auch die Identität eines Rechners über eine Prüfsumme sichergestellt werden kann. Wesentliche Aspekte der Konfiguration des SSH-Servers lassen sich über Univention Configuration Registry anpassen.

Standardmäßig ist der Login des privilegierten `root`-Benutzers per SSH erlaubt (etwa um ein neu installiertes System an einem entfernten Standort zu konfigurieren, auf dem noch keine weiteren Benutzer angelegt wurden).

- Wird die Univention Configuration Registry Variable *sshd/permitroot* (Seite 318) auf `without-password` gesetzt, so wird für den `root`-Benutzer keine interaktive Passwort-Abfrage mehr durchgeführt, sondern beispielsweise nur eine Public-Key-basierte Anmeldung, was Brute-Force-Attacken auf Passwörter vermeidet.
- Soll für den `root`-Benutzer überhaupt keine SSH-Anmeldung mehr möglich sein, kann dies durch Setzen der Univention Configuration Registry Variable *auth/sshd/user/root* (Seite 303) auf `no` deaktiviert werden.

Mit der Univention Configuration Registry Variable *sshd/xforwarding* (Seite 318) kann konfiguriert werden, ob eine X11-Ausgabe über SSH weitergeleitet werden soll. Dies ist u.a. nötig, um einem Benutzer die Möglichkeit zu geben durch einen Login mit **`ssh -X ZIELRECHNER`** ein Programm mit grafischer Ausgabe auf einem entfernten Rechner zu starten. Die möglichen Einstellungen sind `yes` und `no`.

Der Standard-Port für SSH-Verbindungen ist Port 22 über TCP. Wenn ein abweichender Port verwendet werden soll, kann dies über die Univention Configuration Registry-Variable *sshd/port* (Seite 318) konfiguriert werden.

8.4.11 Konfiguration der Zeitzone / Zeitsynchronisation

Die Zeitzone, in der ein System angesiedelt ist, kann im UMC-Modul *Sprach-Einstellungen* unter *Zeitzonen- und Tastatureinstellungen* ▸ *Zeitzone* geändert werden.

Asynchrone Systemzeiten zwischen den einzelnen Rechnern einer Domäne können die Quelle vielfältiger Fehler bedeuten, zum Beispiel:

- Sie verringern beispielsweise die Verlässlichkeit von Log-Dateien.
- Der Kerberos-Betrieb ist gestört.
- Die korrekte Auswertung von Passwortablaufintervallen kann gestört sein.

In einer Domäne dient standardmäßig der Primary Directory Node als Zeitserver. Über die Univention Configuration Registry-Variablen *timeserver* (Seite 319), *timeserver2* (Seite 319) und *timeserver3* (Seite 319) können externe NTP-Server als Zeitquelle eingebunden werden.

Eine manuelle Zeitsynchronisation kann durch den Befehl **ntpdate** gestartet werden.

Windows-Clients, die in eine Samba/AD-Domäne gejoint wurden, akzeptieren nur signierte NTP-Zeitanfragen. Wird die Univention Configuration Registry Variable *ntp/signed* (Seite 314) auf `yes` gesetzt, werden die NTP-Pakete durch Samba/AD signiert.

KAPITEL 9

Services für Windows

UCS kann Active Directory (AD) Dienste anbieten, Mitglied einer Active Directory-Domäne sein oder Objekte zwischen Active Directory-Domänen und einer UCS-Domäne synchronisieren.

Aus Sicht von Windows-Systemen kann UCS die Aufgaben von Windows-Serversystemen übernehmen:

- Domänencontrollerfunktionalität / Authentifizierungsdienste
- Dateidienste
- Druckdienste

Alle diese Dienste werden in UCS durch die Software Samba bereitgestellt.

UCS unterstützt zusätzlich die weitgehend automatische Migration einer bestehenden Microsoft Active Directory Domäne zu UCS. Dabei werden alle Benutzer, Gruppen, Rechnerobjekte und Gruppenrichtlinien übernommen, ohne dass die Windows-Clients erneut der Domäne beitreten müssen. Dies ist in *Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover* (Seite 203) beschrieben.

Microsoft Active Directory-Domänencontroller können aktuell nicht einer UCS-Samba-Domäne beitreten. Diese Funktionalität ist zu einem späteren Zeitpunkt geplant.

Samba kann zum jetzigen Zeitpunkt noch nicht einem Active Directory Forest beitreten.

Eingehende Vertrauensstellungen mit anderen Active Directory Domänen sind konfigurierbar. In dieser Konstellation vertraut die externe Active Directory Domäne den Authentifizierungsentscheidungen der UCS-Domäne (Windows vertraut UCS), so dass sich Benutzer auch an Systemen und Active Directory basierten Diensten in der Windows-Domäne anmelden können (siehe *Vertrauensstellungen* (Seite 208)). Ausgehende Vertrauensstellungen mit Active Directory Domänen (UCS vertraut Windows) sind aktuell nicht unterstützt.

9.1 Betrieb einer Samba-Domäne auf Basis von Active Directory

9.1.1 Installation

Samba als AD-Domänencontroller kann auf allen UCS Directory Nodes mit der Applikation **Active Directory-kompatibler Domänencontroller** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **univention-samba4** installiert werden. Auf den Systemrollen Primary Directory Node und Backup Directory Node muss zusätzlich **univention-s4-connector** installiert werden. Anschließend muss der Befehl **univention-run-join-scripts** aufgerufen werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Ein Datei- und Druckserver kann auf UCS Managed Nodes mit der Applikation **Windows-kompatibler Fileserver** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepakete **univention-samba** installiert werden. Anschließend muss der Befehl **univention-run-join-scripts** aufgerufen werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Samba unterstützt auch den Betrieb als *read-only domain controller*. Die Einrichtung ist in *Extended Windows integration documentation* [7] dokumentiert.

9.1.2 Dienste einer Samba-Domäne

Authentifizierungsdienst

Benutzeranmeldungen können nur auf Microsoft Windows-Systemen erfolgen, die der Samba-Domäne beigetreten sind. Der Domänenbeitritt ist in *Windows-Domänenbeitritt* (Seite 32) dokumentiert.

Benutzer, die sich an einem Windows-System anmelden, erhalten bei der Anmeldung ein Kerberos-Ticket, mit dem die weitere Authentifizierung durchgeführt wird. Mit diesem Ticket wird dann auf die Ressourcen der Domäne zugegriffen.

Häufige Fehlerquellen bei fehlschlagenden Anmeldungen sind:

- Für eine funktionierende Kerberos-Authentifizierung ist eine Synchronisation der Systemzeiten zwischen Windows-Client und Domänencontroller zwingend erforderlich. In der Grundeinstellung wird beim Systemstart die Systemzeit über NTP aktualisiert. Dies kann mit dem Befehl **w32tm /resync** auch manuell erfolgen.
- Während der Anmeldung müssen DNS-Service-Records aufgelöst werden. Der Windows-Client sollte daher als DNS-Nameserver die IP-Adresse des Domänencontrollers verwenden.

Dateidienste

Ein Dateiserver stellt zentral benötigte Dateien über das Netz bereit und ermöglicht es unter anderem Benutzerdaten auf einem zentralen Server zu bündeln.

Die in UCS integrierten Dateidienste unterstützen eine Bereitstellung von Freigaben auf Basis von `CIFS`/`SMB` (siehe *Verwaltung von Freigaben* (Seite 247)). Sofern das unterliegende Dateisystem Access Control Lists (ACLs) unterstützt (verwendbar bei `ext4` und `XFS`) sind ACLs auch von Windows-Clients verwendbar.

Dateidienste können auch von Samba Active Directory-Domänencontrollern, d.h. auf UCS Directory Nodes bereitgestellt werden. Generell wird in Samba-Umgebungen - analog zu den Microsoft-Empfehlungen für Active Directory - empfohlen Domänencontroller- und Datei/Druckdienste zu trennen, d.h. UCS Directory Nodes für die Anmeldung und Managed Nodes für Datei-/Druckdienste zu verwenden. Dies stellt sicher, dass hohe Last auf einem Fileserver nicht zu Störungen im Anmeldedienst führen. Für kleine Umgebungen, in denen keine Möglichkeit für den Betrieb zweier Server gegeben ist, können Datei- und Druckdienste auch mit auf einem Domänencontroller betrieben werden.

Samba unterstützt das `CIFS`-Protokoll und den Nachfolger `SMB2`. Verwendet man einen Client, der `SMB2` unterstützt (ab **Windows Vista**, also auch **Windows 7/8**), verbessert sich die Performance und die Skalierbarkeit.

Das Protokoll kann über die Univention Configuration Registry-Variable *samba/max/protocol* (Seite 316) konfiguriert werden. Sie muss auf allen Samba-Servern gesetzt und anschließend der/die Samba-Server neu gestartet werden.

- `NT1` konfiguriert *CIFS* (unterstützt von allen Windows-Versionen)
- `SMB2` konfiguriert *SMB2* (unterstützt ab **Windows Vista**/**Windows 7**)
- `SMB3` konfiguriert *SMB3* (unterstützt ab **Windows 8**)

Druckdienste

Samba bietet die Möglichkeit, unter Linux eingerichtete Drucker als Netzwerkdrucker für Windows-Clients freizugeben. Die Verwaltung der Druckerfreigaben und die Integration der Druckertreiber ist in *Druckdienste* (Seite 259) beschrieben.

Druckdienste können auch mit Samba AD-Domänencontrollern bereitgestellt werden. Hierbei sind die in *Dateidienste* (Seite 178) beschriebenen Einschränkungen zu beachten.

Univention S4 Connector

Samba stellt einen separaten LDAP-Verzeichnisdienst bereit. Die Synchronisation zwischen dem UCS-LDAP und dem Samba-LDAP erfolgt durch einen internen Systemdienst, den *Univention S4 Connector*. Der Connector ist standardmäßig auf dem Primary Directory Node aktiviert und benötigt normalerweise keine weitere Konfiguration.

Hinweise zum Status der Synchronisation finden sich in der Logdatei `/var/log/univention/connector-s4.log`. Weitere Informationen zur Fehleranalyse von eventuellen Connectorproblemen finden sich in KB 32 - Samba 4 Troubleshooting[38].

Mit dem Befehl **`univention-s4search`** kann im Samba-Verzeichnisdienst gesucht werden. Wird es als Benutzer `root` aufgerufen, werden automatisch die nötigen Credentials des Maschinenkontos verwendet:

```
$ root@primary:~# univention-s4search sAMAccountName=Administrator
# record 1
dn: CN=Administrator,CN=Users,DC=example,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Administrator
instanceType: 4
(..)
```

DRS-Replikation der Verzeichnisdaten

Samba/AD-Domänen verwenden das Directory Replication System (DRS) zur Replikation der Verzeichnisdaten. DRS erlaubt Multimasterreplikation, d.h. die schreibenden Änderungen mehrerer Samba/AD-Domänencontroller werden auf Protokollebene synchronisiert. Die Verwendung von Snapshots in Virtualisierungslösungen sollte daher beim Einsatz von Samba/AD vermieden und Samba/AD auf einem Server betrieben werden, der durchgehend eingeschaltet bleibt.

Mit jedem weiteren Samba/AD-Domänencontroller steigt die Komplexität der Multimasterreplikation. Es sollte daher geprüft werden, ob weitere Samba/AD-Domänencontroller auf Basis von UCS Directory Nodes nötig sind oder für neue Server nicht ein UCS Managed Node die bessere Wahl ist.

Hinweise zur Analyse von DRS-Replikationsproblemen finden sich in KB 32 - Samba 4 Troubleshooting[39].

[38] https://help.univention.com/t/32
[39] https://help.univention.com/t/32

Synchronisation der SYSVOL-Freigabe

Die SYSVOL-Freigabe ist eine Freigabe, die in Active Directory/Samba Gruppenrichtlinien und Anmeldeskripte bereitstellt. Sie wird zwischen allen Domänencontrollern synchronisiert und im Verzeichnis `/var/lib/samba/sysvol/` gespeichert.

In Microsoft Active Directory wird die SYSVOL-Freigabe durch den File Replication Service (eingeführt mit Windows 2000) oder durch das Distributed File System (ab Windows 2008 R2) synchronisiert. Diese Replikationsmethoden sind in Samba noch nicht vollständig implementiert. Die Synchronisation zwischen den Samba/AD-Domänencontrollern erfolgt in UCS durch einen Cron-Job (standardmäßig alle fünf Minuten, konfigurierbar durch die Univention Configuration Registry Variable *samba4/sysvol/sync/cron* (Seite 317)).

9.1.3 Konfiguration und Management von Windows-Desktops

Gruppenrichtlinien

Gruppenrichtlinien sind eine Active Directory-Funktion, die die zentrale Konfiguration von Vorgaben für Rechner und Benutzer erlaubt. Gruppenrichtlinien werden auch von Samba/AD-Domänen unterstützt. Die Richtlinien greifen nur auf Windows-Clients; Linux- oder Mac OS-Systeme werten die Richtlinien nicht aus.

Gruppenrichtlinien werden ausgehend von der englischen Bezeichnung *Group policy objects* auch oft als GPOs bezeichnet. Genauer gesagt kann ein Gruppenrichtlinienobjekt eine Reihe von Richtlinien beinhalten. Trotz ihres Namens lassen sich Gruppenrichtlinienobjekte nicht direkt bestimmten Benutzergruppen zuweisen, sondern sie werden vielmehr mit bestimmten AD-Verwaltungseinheiten (Domänen, Sites oder Organisationseinheiten) im Samba-Verzeichnisdienst (Samba AD/DS) verknüpft und beziehen sich dadurch auf untergeordnete Objekte. Eine gruppen- oder benutzerspezifische Auswertung ist nur indirekt über die *Sicherheitseinstellungen* eines Gruppenrichtlinienobjekts möglich, in denen sich das Recht *Gruppenrichtlinie übernehmen* gezielt auf bestimmte Gruppen, Benutzer oder Computer einschränken lässt.

Grundsätzlich sind die *Gruppenrichtlinien* (*Group Policies* (GPO)) von den sehr ähnlich benannten *Gruppenrichtlinieneinstellungen* (*Group Policy Preferences* (GPP)) zu unterscheiden:

- Die über *Gruppenrichtlinien* (GPOs) getroffenen Vorgaben sind bindend, während sich über *Gruppenrichtlinieneinstellungen* (GPPs) nur Präferenzen in die Registry von Windows-Clients eintragen lassen, die aber unter Umständen am Client überschrieben werden können.
- Die über *Gruppenrichtlinien* (GPOs) getroffenen Vorgaben werden zudem dynamisch auf die Zielobjekte angewendet, wo hingegen die über *Gruppenrichtlinieneinstellungen* (GPPs) getroffenen Einstellungen statisch in die Registry von Windows-Clients eintragen werden (man spricht hier auch von *Tattooing*).

Aus diesen Gründen sind *Gruppenrichtlinien* (GPOs) in den meisten Fällen den *Gruppenrichtlinieneinstellungen* (GPPs) vorzuziehen. Dieses Kapitel bezieht sich im weiteren ausschließlich auf *Gruppenrichtlinien* (GPOs).

Gruppenrichtlinien werden im Gegensatz zu den UCS-Richtlinien (siehe *Richtlinien* (Seite 77)) nicht über UMC-Module, sondern mit einem separaten Editor konfiguriert, mit der *Gruppenrichtlinienverwaltung*, die Teil der *Remote Server Administration Tools* (RSAT) ist. Die Einrichtung ist in *Installation der Gruppenrichtlinienverwaltung* (Seite 181) dokumentiert.

Es existieren zwei Arten von Richtlinien:

Benutzerrichtlinien
: *Benutzerrichtlinien* konfigurieren die Einstellungen eines Benutzers, z.B. die Vorkonfiguration des Desktops. Auch Anwendungen können über Gruppenrichtlinien konfiguriert werden (z.B. die Startseite des Browsers oder Einstellungen in LibreOffice).

Computer-Richtlinien
: *Computer-Richtlinien* definieren die Einstellungen von Windows-Clients.

Computerrichtlinien werden erstmals beim Systemstart ausgewertet, Benutzerrichtlinien bei der Anmeldung. Die Richtlinien werden auch für angemeldete Benutzer/laufende Systeme fortlaufend ausgewertet und aktualisiert (in der Grundeinstellung alle 90-120 Minuten, der Zeitraum wird zur Vermeidung von Lastspitzen nach dem Zufallsprinzip variiert).

Die Auswertung der Gruppenrichtlinien kann durch Aufruf des Befehls **`gpupdate /force`** auch gezielt gestartet werden.

Einige Richtlinien - z.B. zur Installation von Software oder für Anmeldeskripte - werden nur bei der Anmeldung (Benutzerrichtlinien) oder beim Systemstart (Rechnerrichtlinien) ausgewertet.

Die meisten Gruppenrichtlinien setzen nur einen Wert in der Windows-Registry, der dann von Windows oder einer Applikation ausgewertet wird. Da Standardbenutzer keine Einstellungen in dem entsprechenden Teil der Windows Registry editieren können, können so auch eingeschränkte Benutzer-Desktops konfiguriert werden, in denen z.B. Benutzer den Windows Task Manager nicht aufrufen dürfen.

Die Gruppenrichtlinien werden in der SYSVOL-Freigabe gespeichert, siehe *Synchronisation der SYSVOL-Freigabe* (Seite 180). Sie werden mit Benutzer- und Rechnerkonten im Samba-Verzeichnisdienst verknüpft.

Installation der Gruppenrichtlinienverwaltung

Die **`Gruppenrichtlinienverwaltung`** kann als Teil der *Remote Server Administration Tools* auf Windows Clients installiert werden. Sie können für Windows 10 unter Remote Server Administration Tools (RSAT) for Windows 10[40] bezogen werden.

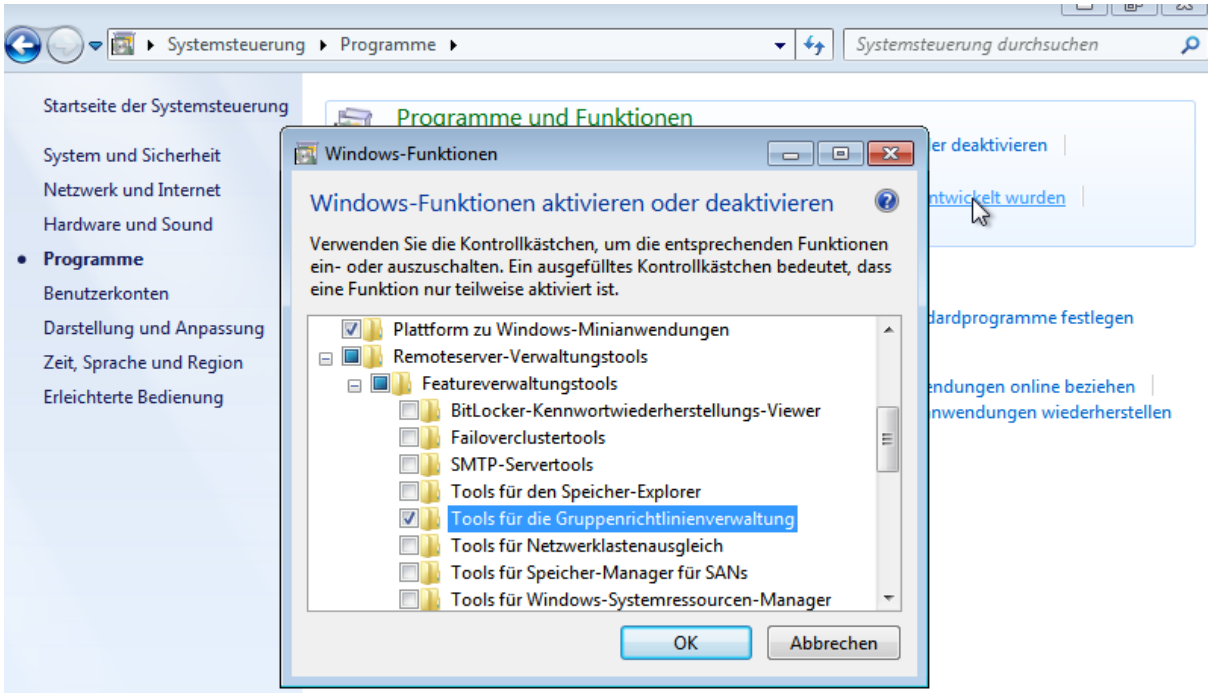


Abb. 9.1: Aktivierung der Gruppenrichtlinienverwaltung

Nach der Installation muss die Gruppenrichtlinienverwaltung in der Windows-Systemsteuerung noch aktiviert werden, in dem unter *Start ▸ Systemsteuerung ▸ Programme ▸ Windows-Funktionen aktivieren und deaktivieren ▸ Remoteserver-Verwaltungstools ▸ Featureverwaltungs-Tools* die Option *Tools für die Gruppenrichtlinienverwaltung* aktiviert wird.

Nach der Aktivierung kann die Gruppenrichtlinienverwaltung unter *Start ▸ Verwaltung ▸ Gruppenrichtlinienverwaltung* aufgerufen werden.

[40] https://www.microsoft.com/en-us/download/details.aspx?id=45520

Konfiguration von Richtlinien mit der Gruppenrichtlinienverwaltung

Gruppenrichtlinien können nur von Benutzern konfiguriert werden, die Mitglied der Gruppe `Domain Admins` sind (z.B. der `Administrator`). Bei der Anmeldung muss beachtet werden, dass keine Anmeldung mit dem lokalen Administrator-Konto erfolgt, sondern mit dem Administrator-Konto der Domäne. Die Gruppenrichtlinienverwaltung kann auf einem beliebigen System der Domäne aufgerufen werden.

Wenn mehr als ein Samba-Domänencontroller eingesetzt wird, muss die Replikation der GPO-Daten berücksichtigt werden, siehe *Konfiguration von Gruppenrichtlinien in Umgebungen mit mehr als einem Samba-Domänencontroller* (Seite 185).

Es gibt zwei prinzipielle Möglichkeiten GPOs zu erstellen:

- Sie können im *Gruppenrichtlinienobjekte*-Order angelegt und dann mit verschiedenen Positionen im LDAP verknüpft werden. Dies ist sinnvoll, wenn eine Richtlinie mit mehreren Positionen im LDAP verknüpft werden soll.
- Die GPO kann ad hoc an einer LDAP-Position erstellt und dabei direkt verknüpft werden. Für kleine und mittlere Domänen ist das der einfachere Weg. Auch ad hoc erstellte Domänen werden im *Gruppenrichtlinienobjekte*-Ordner angezeigt.

Eine Richtlinie kann drei Zustände annehmen; sie kann `aktiviert`, `deaktiviert` oder `nicht gesetzt` sein. Die Auswirkung bezieht sich immer auf die Formulierung der Richtlinie. Wenn diese beispielsweise *Deaktiviere Feature xy* heißt, muss die Richtlinie aktiviert werden um das Feature abzuschalten. Einige Richtlinien haben zusätzliche Optionen, z.B. könnte die Richtlinie *Aktiviere Mail-Quota* eine zusätzliche Option mitbringen um die Speichermenge zu verwalten.

Zwei Standard-Richtlinienobjekte sind vordefiniert:

Default Domain Policy
: Das *Default Domain Policy* Objekt kann verwendet werden, um globale Richtlinien für alle Benutzer und Rechner der gesamten Domäne zu konfigurieren.

Default Domain Controllers Policy
: Das *Default Domain Controllers Policy* Objekt hat in einer Samba-Domäne keine Verwendung (in einer Microsoft AD-Domäne würden die Richtlinien für Microsoft-Domänencontroller über dieses Objekt erfolgen). Die Konfiguration der Samba-Domänencontroller erfolgt in UCS weitgehend über Univention Configuration Registry.

AD-Domänen können in Sites strukturiert werden. Dies kann z.B. verwendet werden um Standorte in einer Domäne zu gruppieren. Im Hauptmenü der Gruppenrichtlinienverwaltung werden alle Sites aufgeführt. Dort findet sich auch eine Liste von Domänen. Die aktuellen Samba-Versionen unterstützen keine Forest-Domänen, so dass hier immer nur eine Domäne angezeigt wird.

Eine Domäne kann in verschiedene Organisationseinheiten (OUs) strukturiert werden. Dies kann z.B. verwendet werden, um die Mitarbeiter der Buchhaltung und die Benutzer der Verwaltung in unterschiedlichen LDAP-Positionen zu speichern.

Gruppenrichtlinien können sich gegenseitig überlagern. Es gilt das Prinzip der Vererbung, d.h. höherliegende Richtlinien überschreiben die untergeordneten. Die effektiven Richtlinien für einen Benutzer können sowohl mit dem Modellierungsassistenten der *Gruppenrichtlinienverwaltung* als auch an der Windows-Kommandozeile mit dem Befehl **`gpresult /user BENUTZERNAME /v`** auf dem Windows-Client angezeigt werden.

Die Richtlinien werden in folgender Reihenfolge ausgewertet:

1. Richtlinien der *Default Domain Policy* gelten als Grundeinstellung für alle Benutzer und Rechner der gesamten Domäne.
2. Mit einer OU verknüpfte Richtlinien überschreiben Richtlinien aus der Default Domain Policy. Sind OUs weiter verschachtelt, greifen im Konfliktfall die jeweils „untersten“ Richtlinien, d.h. die, die näher am Zielobjekt verknüpft sind. Es gilt folgende Auswertungsreihenfolge:
   - Zuweisung einer Richtlinie zu einem Active Directory Standort
   - Vorgaben der Default Domain Policy

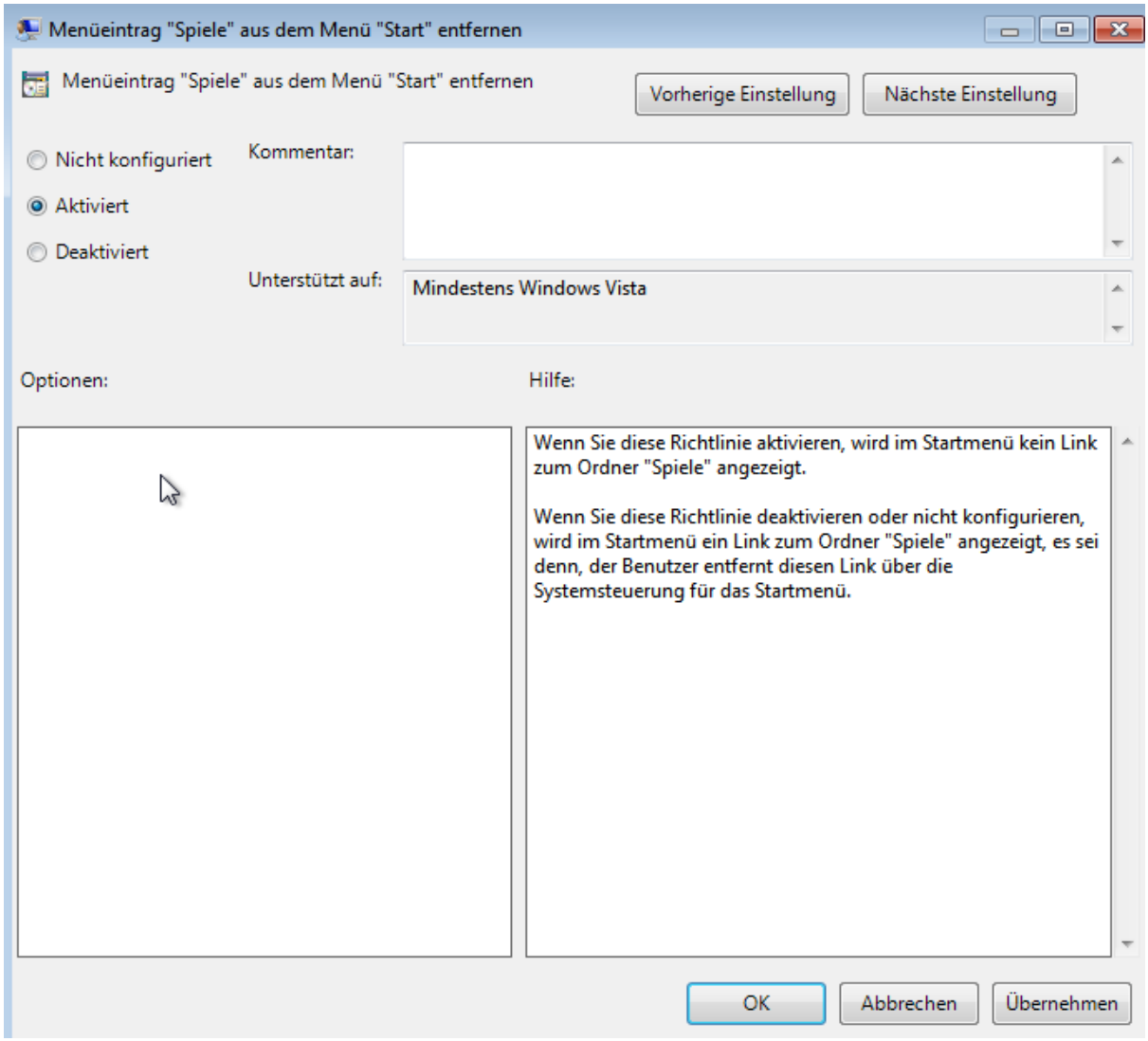


Abb. 9.2: Bearbeiten einer Richtlinie

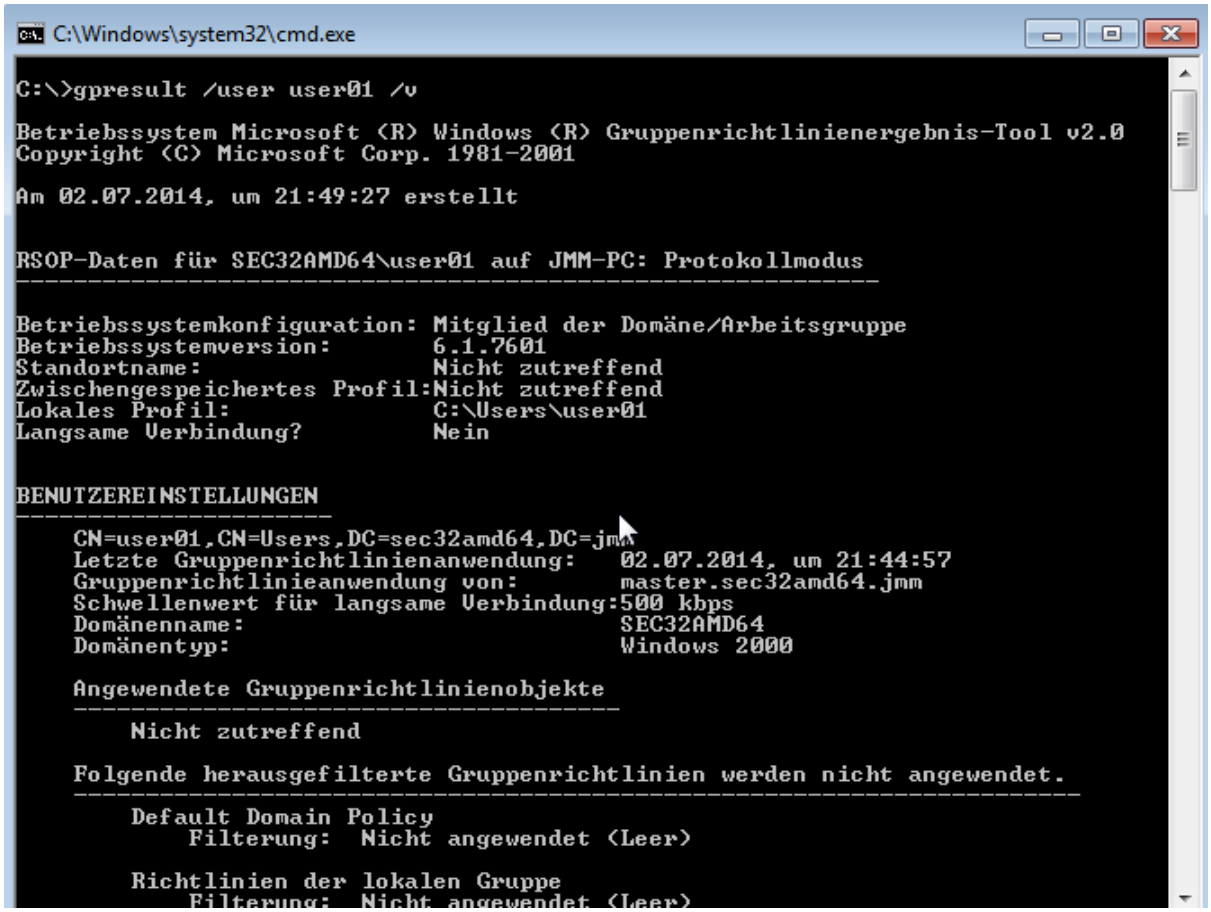


Abb. 9.3: Auswertung der GPO für den Benutzer `user01`

- Zuweisung einer Richtlinie zu einer Organisationseinheit / OU (jede unterliegende OU überstimmt wiederum Richtlinien aus übergeordneten OUs).

Ein Beispiel: Eine Firma verbietet allgemein den Zugriff auf den **`Windows Task Manager`**. Dazu wird im *Default Domain Policy*-Objekt die Richtlinie *Zugriff auf Task Manager unterbinden* aktiviert. Für einige technisch versierte Benutzer soll der Task Manager dennoch verfügbar sein. Diese Benutzer sind in der OU *Technik* abgelegt. Nun wird ein zusätzliches Gruppenrichtlinienobjekt angelegt, in dem Richtlinie *Zugriff auf Task Manager unterbinden* auf *deaktiviert* gesetzt wird. Dieses neue GPO wird mit der OU *Technik* verbunden.

Konfiguration von Gruppenrichtlinien in Umgebungen mit mehr als einem Samba-Domänencontroller

Eine Gruppenrichtlinie besteht technisch aus zwei Teilen: Zum einen gibt es ein Verzeichnis im Dateisystem der Domänencontroller, das die eigentlichen Richtlinien-Dateien enthält, die auf dem Windows-System umgesetzt werden sollen (gespeichert in der SYSVOL-Freigabe (siehe *Synchronisation der SYSVOL-Freigabe* (Seite 180))). Zum anderen gibt es ein gleichnamiges Objekt im LDAP-Baum des Samba-Verzeichnisdienstes (Samba AD/DS), das üblicherweise unter einem LDAP-Container namens *Group Policy Objects* abgelegt ist.

Während die LDAP-Replikation zwischen Domänencontrollern innerhalb weniger Sekunden umgesetzt ist, werden die Dateien in der SYSVOL-Freigabe in der Grundeinstellung nur alle fünf Minuten repliziert. Es ist zu beachten, dass die Anwendung von neu konfigurierten Gruppenrichtlinien in diesem Zeitraum fehlschlagen kann, falls ein Client zufällig einen Domänencontroller konsultiert, der noch nicht die aktuellen Dateien zu sich repliziert hat.

Administrative Vorlagen (ADMX/ADM)

Die in der *Gruppenrichtlinienverwaltung* angezeigten Richtlinien können durch sogenannte *Administrative Vorlagen* erweitert werden. In einer solchen Vorlage wird definiert, unter welchem Namen die Richtlinie in der Gruppenrichtlinienverwaltung erscheinen soll und welcher Wert dadurch in der Windows-Registry gesetzt wird. Administrative Vorlagen werden in sogenannten *ADMX-Dateien* (früher *ADM-Dateien*) gespeichert, siehe *Group Policy ADMX Syntax Reference Guide* [8].

ADMX-Dateien bieten unter anderem den Vorteil, dass sie zentral über mehrere Domänencontroller bereitgestellt werden können, damit die Gruppenrichtlinienverwaltung an allen Windows-Clients die gleichen Konfigurationsmöglichkeiten zeigt, siehe *How to Implement the Central Store for Group Policy Admin Templates, Completely (Hint: Remove Those .ADM files!)* [9].

Das folgende Beispiel für eine ADM-Datei definiert eine Rechner-Richtlinie, in der ein Registry-Key des (fiktiven) Univention RDP-Client konfiguriert wird. ADM-Dateien können über Drittwerkzeuge in das neuere ADMX-Format umgewandelt werden. Die administrativen Vorlagen müssen die Dateiendung `.adm` verwenden:

```
CLASS MACHINE
CATEGORY "Univention"
POLICY "RDP-Client"
KEYNAME "Univention\RDP\StorageRedirect"
EXPLAIN "Ist diese Option aktiviert, wird Soundausgabe im RDP-Client aktiviert"
VALUENAME "Sound-Weiterleitung"
VALUEON "Aktiviert"
VALUEOFF "Deaktiviert"
END POLICY
END CATEGORY
```

Die ADM-Datei kann anschließend in das ADMX-Format umgewandelt oder aber direkt über die Gruppenrichtlinienverwaltung importiert werden. Dazu wird im Kontextmenü *Administrativen Vorlagen* ▸ *Vorlagen hinzufügen* ▸ *entfernen* aufgerufen. Mit *Hinzufügen* kann dann eine ADM-Datei importiert werden. Die administrativen Vorlagen werden ebenfalls in der SYSVOL-Freigabe gespeichert und repliziert, wodurch die Gruppenrichtlinienverwaltung von den Windows-Clients aus auf sie zugreifen kann.

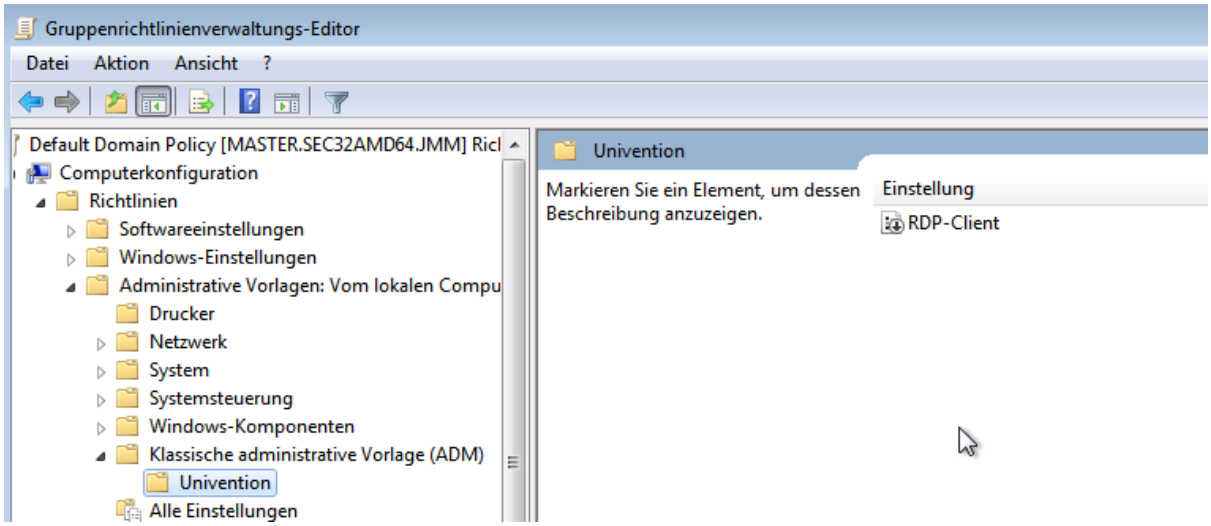


Abb. 9.4: Die eingebundene administrative Vorlage

Anwendung von Richtlinien auf Basis von Rechnereigenschaften (WMI-Filter)

Richtlinien können auch auf Basis von Systemeigenschaften konfiguriert werden. Diese Eigenschaften werden über die Windows Management Instrumentation-Schnittstelle (WMI) bereitgestellt. Der darauf aufbauende Mechanismus wird als *WMI-Filterung* bezeichnet. Damit ist es beispielsweise möglich, eine Richtlinie nur auf PCs mit einer 64 Bit-Prozessor-Architektur oder mit mindestens 8 GB RAM anzuwenden. Ändert sich eine Eigenschaft eines Systems (z.B. weil mehr Speicher eingebaut wurde), wird der jeweilige Filter automatisch vom Client neu ausgewertet.

Die WMI-Filter werden in der Domänenstruktur im Container *WMI-Filter* angezeigt. Mit *Neu* kann ein weiterer Filter definiert werden. Unter *Abfragen* werden die Filterregeln definiert. Die Regeln werden in einer SQL-ähnlichen Syntax definiert. Regel-Beispiele finden sich in Microsoft [10] und Heitbrink [11].

Anmeldeskripte / NETLOGON-Freigabe

Die NETLOGON-Freigabe dient der Bereitstellung von Anmeldeskripten in Windows-Domänen. Die Anmeldeskripte werden nach der erfolgreichen Anmeldung eines Benutzers ausgeführt und ermöglichen die Anpassung der Arbeitsumgebung des Benutzers. Die Skripte müssen in einem für Windows ausführbaren Format gespeichert werden, wie z.B. `bat`.

Die Anmeldeskripte werden unter `/var/lib/samba/sysvol/`*`Domänenname`*`/scripts/` abgelegt und unter dem Freigabennamen *NETLOGON* bereitgestellt. Der Dateiname des Skripts muss relativ zu diesem Verzeichnis angegeben werden.

Die NETLOGON-Freigabe wird im Rahmen der SYSVOL-Replikation repliziert.

Das Anmeldeskript kann pro Benutzer zugewiesen werden, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110).

Konfiguration des Servers, auf dem das Heimatverzeichnis abgelegt wird

Das Heimatverzeichnis wird benutzerbezogen im UMC-Modul *Benutzer* definiert, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110). Dies erfolgt mit der Einstellung *Windows-Heimatverzeichnis*, z.B. `\ucs-file-servermeier`.

Für das Zuweisen des Heimatverzeichnis-Servers an mehrere Benutzer auf einmal kann der Mehrfachbearbeitungsmodus von UMC-Modulen verwendet werden, siehe *Bearbeiten von Objekten* (Seite 75).

Servergespeicherte Profile

Samba unterstützt servergespeicherte Profile, d.h. Einstellungen der Benutzer werden auf einem Server gespeichert. In diesem Verzeichnis werden auch die Dateien gespeichert, die der Benutzer im Ordner *Eigene Dateien* speichert. Sie werden zwischenzeitlich lokal auf dem Windows-Rechner vorgehalten und erst bei der Abmeldung auf den Samba-Server synchronisiert.

In Samba-Domänen mit Active Directory-Support werden in der Voreinstellung keine serverseitigen Profile verwendet.

Das Profilverzeichnis kann über eine Gruppenrichtlinie konfiguriert werden, die unter *Computerkonfiguration ‣ Richtlinien ‣ Administrative Vorlagen ‣ System ‣ Benutzerprofile ‣ Pfad des servergespeicherten Profils für alle Benutzer festlegen* zu finden ist. Wenn hier z.B. der *UNC*-Pfad `%LOGONSERVER%\%USERNAME%\windows-profiles\default` eingetragen wird, dann werden die Verzeichnisse `windows-profiles\default.V?` im Heimatverzeichnis des Benutzers auf dem jeweils gewählten Logonserver verwendet.

Alternativ kann das Profilverzeichnis individuell für einzelne Benutzerkonten definiert werden. Das ist im UMC-Modul *Benutzer* unter dem Reiter *Konto* des Benutzerkontos über das Feld *Profilverzeichnis* möglich. Der entsprechende UDM-Attributname heißt `profilepath`. Mit OpenLDAP als Backend wird dies im LDAP-Attribut `sambaProfilePath` gespeichert.

Wird der Profilpfad geändert, wird ein neues Profilverzeichnis angelegt. Die Daten aus dem alten Profilverzeichnis bleiben dabei erhalten und können manuell in das neue Profilverzeichnis kopiert beziehungsweise verschoben werden. Abschließend kann das alte Profilverzeichnis gelöscht werden.

Bemerkung: Der Administrator-Benutzer greift standardmäßig mit root-Berechtigungen auf Freigaben zu. Wenn dadurch das Profilverzeichnis mit root als Benutzer angelegt wird, sollte es manuell mit dem Befehl **`chown`** an den Administrator vergeben werden.

9.2 Active Directory-Verbindung

Univention Corporate Server kann auf zwei unterschiedliche Arten mit einer bestehenden Active Directory-Domäne (AD-Domäne) zusammen betrieben werden. Beide Varianten lassen sich durch die Applikation **`Active Directory-Verbindung`** aus dem Univention App Center einrichten (siehe *Installation weiterer Software* (Seite 104)). Diese steht auf einem Primary Directory Node und Backup Directory Node zur Verfügung.

Die beiden Varianten sind:

- UCS als Teil (Domänen-Mitglied) einer AD-Domäne (siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 188))
- Synchronisation von Kontendaten zwischen einer AD-Domäne und einer UCS-Domäne (siehe *Einrichtung des UCS AD-Connectors* (Seite 191)).

In beiden Modi wird unter UCS der Dienst **`Active Directory-Verbindung`** verwendet (kurz UCS AD-Connector), der Verzeichnisdienstobjekte zwischen einem Microsoft Windows Server mit Active Directory (AD) und dem OpenLDAP-Verzeichnis aus Univention Corporate Server synchronisieren kann.

Im ersten Fall, der Konfiguration eines UCS-Serversystems als Mitglied einer AD-Domäne, dient das AD als führender Verzeichnisdienst und das jeweilige UCS-System tritt dem Vertrauenskontext der AD-Domäne bei. Durch

die Domänenmitgliedschaft hat das UCS-System limitierten Zugriff auf Kontodaten der Active Directory-Domäne. Die Einrichtung dieses Betriebsmodus ist im Detail in *UCS als Mitglied einer Active Directory-Domäne* (Seite 188) beschrieben.

Der zweite Modus, der sich über die App *Active Directory-Verbindung* konfigurieren lässt, dient dazu, die UCS Domäne parallel zu einer bestehenden AD-Domäne zu betreiben. In diesem Modus ist jedem Domänen-Benutzer sowohl in der UCS- als auch in der AD-Domäne ein gleichnamiges Benutzerkonto zugeordnet. Durch die Namensidentität und die Synchronisation der verschlüsselten Passwortdaten ermöglicht dieser Modus einen transparenten Zugriff zwischen beiden Domänen. Die Authentifikation eines Benutzers in der UCS-Domäne geschieht in diesem Modus direkt innerhalb der UCS-Domäne und ist damit nicht direkt abhängig von der AD-Domäne. Die Einrichtung diese Betriebsmodus ist im Detail in *Einrichtung des UCS AD-Connectors* (Seite 191) beschrieben.

9.2.1 Unterstütze Windows-Versionen in *AD-Verbindung*

`Active Directory Connection` unterstützt Microsoft Windows Server in den Versionen 2012, 2016, 2019 und 2022.

9.2.2 UCS als Mitglied einer Active Directory-Domäne

Bei der Konfiguration eines UCS-Serversystems als Mitglied einer AD-Domäne (*AD member*-Modus) dient das AD als führender Verzeichnisdienst und das jeweilige UCS-System tritt dem Vertrauenskontext der AD-Domäne bei. Das UCS-System ist nicht in der Lage selbst als Active Directory Domänencontroller zu arbeiten. Durch die Domänenmitgliedschaft hat das UCS-System limitierten Zugriff auf Kontodaten der Active Directory-Domäne, die es über den UCS AD-Connector aus dem AD ausliest und lokal in den eigenen OpenLDAP-basierten Verzeichnisdienst schreibt. In dieser Konfiguration schreibt der UCS AD-Connector keine Änderungen in das AD.

Der *AD Member*-Modus eignet sich, um eine AD-Domäne durch Applikationen zu erweitern, die auf der UCS-Plattform zur Verfügung stehen. Auf der UCS-Plattform installierte Apps sind dann für Benutzer der AD-Domäne nutzbar. Die Authentifikation erfolgt dabei weiter gegen native Microsoft AD-Domänencontroller.

Der Einrichtungsassistent kann direkt bei der UCS Installation durch die Auswahl *Einer bestehenden Active-Directory-Domäne beitreten* gestartet werden. Nachträglich kann der Einrichtungsassistent mit der Applikation **`Active Directory-Verbindung`** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **`univention-ad-connector`** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Bemerkung:

- Der *AD member*-Modus kann nur auf einem Primary Directory Node konfiguriert werden.
- Der Name der DNS-Domäne des UCS-Systems muss mit dem der AD-Domäne übereinstimmen. Die Hostnamen selbst müssen natürlich unterschiedlich sein.
- Alle AD- und UCS-Server in einer Connector-Umgebung sollten dieselbe Zeitzone verwenden.

Im ersten Dialog des Einrichtungsassistenten ist der Punkt *UCS als Teil einer AD-Domäne konfigurieren* vorausgewählt und kann mit *Weiter* bestätigt werden.

Im nächsten Dialog wird die Adresse eines AD-Domänencontrollers sowie der Name des Standard-Administrator-Kontos der AD-Domäne und dessen Passwort abgefragt. Hier sollte das Standard AD Administrator-Konto verwendet werden. Der angegebene AD-Domänencontroller muss auch DNS-Dienste für die Domäne bereitstellen. Durch Betätigen der Schaltfläche *AD-Domäne beitreten* wird der Domänenbeitritt gestartet.

Falls die Systemzeit des UCS-Systems mehr als 5 Minuten gegenüber der Systemzeit des AD-Domänencontrollers vorgeht, ist eine manuelle Angleichung der Systemzeiten notwendig. Dies ist notwendig, da die AD-Kerberos-Infrastruktur zur Authentifizierung verwendet wird. Systemzeiten sollten dabei nicht zurückgestellt werden, um Inkonsistenzen zu vermeiden.

Der Domänenbeitritt läuft automatisch ab. Der abschließende Dialog sollte mit *Fertigstellen* bestätigt werden. Danach sollte mit einem Klick auf *Neustart* der UMC-Server neu gestartet werden.

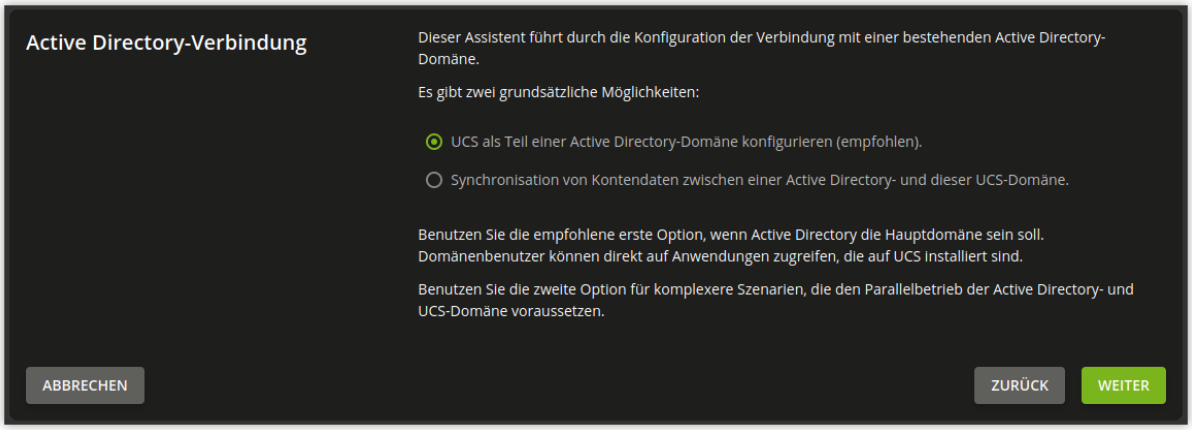


Abb. 9.5: Konfiguration des Betriebsmodus als Teil einer AD-Domäne

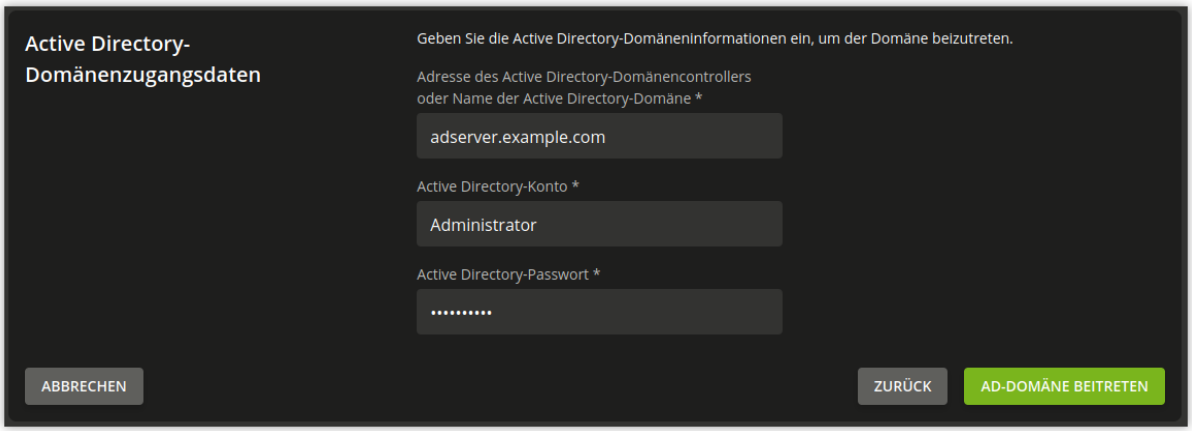


Abb. 9.6: Domänenbeitritt zu einer AD-Domäne

Bemerkung: Nach Einrichtung des *AD member*-Modus findet die Authentifikation gegen den AD-Domänencontroller statt. **Daher gilt für den Administrator jetzt das Passwort aus der AD-Domäne.** Falls einer AD-Domäne mit nicht-englischsprachiger Sprachkonvention beigetreten wurde, dann wird das `Administrator`-Konto aus UCS während des Domänenbeitritts automatisch in die Schreibweise des AD umbenannt. Gleiches gilt für alle Benutzer- und Gruppenobjekte mit *Well Known SID* (z.B. `Domain Admins`).

Warnung: Falls zuvor neben dem Primary Directory Node weitere UCS-Systeme schon Teil der UCS-Domäne waren, dann müssen diese der Domäne neu beitreten. Dabei erkennen sie, dass der Primary Directory Node sich im *AD member*-Modus befindet und treten ebenfalls der Authentifikationsstruktur der AD-Domäne bei und können dann z.B. zusätzlich Samba-Dateifreigaben bereitstellen.

Bemerkung: Da in diesem Modus die AD-Kerberos-Infrastruktur zur Authentifizierung von Benutzern verwendet wird, ist es essenziell, dass die Systemzeiten von UCS und AD-Domänencontroller synchron sind (mit einer Toleranz von 5 Minuten). Zu diesem Zweck ist unter UCS der AD-Domänencontroller als NTP-Zeitserver konfiguriert. Im Falle von Authentifikationsproblemen sollte immer als erstes die Systemzeit überprüft werden.

Nach dieser Einrichtung kann das UMC-Modul *Active Directory-Verbindung* zur weiteren Administration verwendet werden, z.B. um zu prüfen, ob der Dienst läuft und ihn gegebenenfalls neu zu starten (siehe *Start/Stopp des Active Directory Connectors* (Seite 195)).

Um eine verschlüsselte Verbindung zwischen Active Directory und Primary Directory Node nicht nur für die Authentifikation, sondern auch für den Datenaustausch an sich zu verwenden, kann auf dem AD-Domänencontroller das Root-Zertifikat der Zertifizierungsstelle exportiert und über das UMC-Modul hochgeladen werden. Weitere Informationen dazu liefert *Import des SSL-Zertifikats des Active Directory* (Seite 194).

Per Voreinstellung überträgt die so eingerichtete Active Directory-Verbindung keine Passwortdaten aus AD in den UCS-Verzeichnisdienst. Einige Apps aus dem App Center benötigen verschlüsselte Passwortdaten. Sofern eine App diese benötigt, wird ein entsprechender Hinweis im App Center angezeigt.

Im *AD member*-Modus liest der UCS AD-Connector Objektdaten per Voreinstellung mit den Berechtigungen des Maschinenkontos des Primary Directory Nodes aus dem AD. Für das Auslesen von verschlüsselten Passwortdaten sind dessen Berechtigungen nicht ausreichend. Daher muss in diesem Fall zusätzlich manuell die LDAP-DN eines privilegierten Replikationsbenutzers in die Univention Configuration Registry Variable *connector/ad/ldap/binddn* (Seite 303) eingetragen werden. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Passwort muss auf dem Primary Directory Node in eine Datei gespeichert werden und ihr Dateiname muss in die Univention Configuration Registry Variable *connector/ad/ldap/bindpw* (Seite 303) eingetragen werden. Falls zu einem späteren Zeitpunkt das Zugriffspasswort geändert wurde, muss das neue Passwort in diese Datei eingetragen werden. Die Zugriffsrechte für die Datei sollten so eingeschränkt werden, dass nur der Besitzer `root` Zugriff hat.

Die folgenden Kommandos zeigen die Schritte beispielhaft:

```
$ ucr set connector/ad/ldap/binddn=Administrator
$ ucr set connector/ad/ldap/bindpw=/etc/univention/connector/password
$ touch /etc/univention/connector/password
$ chmod 600 /etc/univention/connector/password
$ echo -n "Administrator password" > /etc/univention/connector/password
$ ucr set connector/ad/mapping/user/password/kinit=false
```

Falls gewünscht, kann zu einem späteren Zeitpunkt der AD-Domänencontroller auch durch den Primary Directory Node abgelöst werden. Dies ist über die Applikation *Active Directory Takeover* möglich (siehe *Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover* (Seite 203)).

9.2.3 Einrichtung des UCS AD-Connectors

Als Alternative zur Mitgliedschaft in einer AD-Domäne, die im vorherigen Abschnitt beschrieben ist, kann der UCS Active Directory-Connector dazu verwendet werden, Benutzer- und Gruppenobjekte zwischen einer UCS-Domäne und einer AD-Domäne zu synchronisieren. Diese Betriebsart erlaubt über die unidirektionale Synchronisation hinaus auch die bidirektionale Synchronisation. In dieser Betriebsart bestehen beide Domänen parallel und ihre Authentifikationssysteme funktionieren unabhängig. Dieser Betriebsmodus setzt die Synchronisation verschlüsselter Passwortdaten voraus.

In der Standardeinstellung werden Container, Organisationseinheiten, Benutzer, Gruppen und Rechner synchronisiert.

Der UCS AD Connector kann nur auf einem Primary Directory Node oder einem Backup Directory Node installiert werden.

Hinweise zu den in der Grundeinstellung konfigurierten Attributen und zu beachtende Besonderheiten finden sich in *Details zur vorkonfigurierten Synchronisation* (Seite 202).

Durch die in beiden Domänen gleichen Benutzereinstellungen können Benutzer transparent auf Dienste beider Umgebungen zugreifen. Nachdem eine Domänenanmeldung an einer UCS-Domäne durchgeführt wurde, ist anschließend eine Verbindung zu einer Dateifreigabe oder einem Exchange-Server mit Active Directory ohne erneute Passwortabfrage möglich. Auf den Ressourcen der anderen Domäne finden Benutzer und Administratoren gleichnamige Benutzer und Gruppen vor und können so mit den gewohnten Rechtestrukturen arbeiten.

Nach dem erstmaligen Start des Connectors wird die Initialisierung vorgenommen. Dabei werden alle Einträge aus dem UCS gelesen und entsprechend dem eingestellten Mapping in AD-Objekte umgewandelt und auf AD-Seite hinzugefügt, und, falls bereits vorhanden, modifiziert. Anschließend werden alle Objekte aus dem AD gelesen und in UCS-Objekte umgewandelt und entsprechend auf UCS-Seite hinzugefügt oder modifiziert. Solange noch Änderungen vorliegen, werden die Verzeichnisdienst-Server weiter abgefragt. Der UCS AD-Connector kann auch in einem unidirektionalen Modus betrieben werden.

Nach dem initialen Sync werden weitere Änderungen in einem festen Intervall abgefragt. Dieser Wert ist auf fünf Sekunden eingestellt und kann manuell per Univention Configuration Registry-Variable `connector/ad/poll/sleep` (Seite 304) angepasst werden.

Sollte ein Objekt nicht synchronisiert werden können, so wird dieses Objekt zunächst zurückgestellt (*rejected*). Nach einer konfigurierbaren Anzahl von Durchläufen - das Intervall kann im per Univention Configuration Registry-Variable `connector/ad/retryrejected` (Seite 304) angepasst werden - wird erneut versucht diese Änderungen wieder einzuspielen. Der Standardwert beträgt zehn Durchläufe. Außerdem wird bei einem Neustart des UCS AD-Connectors ebenfalls versucht, die zuvor zurückgewiesenen Änderungen erneut zu synchronisieren.

Grundkonfiguration des UCS AD-Connectors

Der UCS AD-Connector wird über einen Assistenten im UMC-Modul *Active Directory-Verbindung* konfiguriert.

Das Modul kann mit der Applikation **`Active Directory-Verbindung`** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **`univention-ad-connector`** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Bemerkung: Alle AD- und UCS-Server in einer Connector-Umgebung müssen dieselbe Zeitzone verwenden.

Warnung: Trotz intensiver Tests kann aufgrund der Vielfalt der Konfigurations- und Betriebsvarianten einer AD-Domäne nicht ausgeschlossen werden, dass die Ergebnisse des Synchronisationsvorgangs den Betrieb einer produktiven Domäne beeinträchtigen. Der UCS AD-Connector sollte daher vorab in einer getrennten Umgebung auf die jeweiligen Anforderungen geprüft werden.

Es ist zu empfehlen, die folgenden Schritte mit einem Webbrowser vom AD-Domänencontroller aus durchzuführen, da Dateien auf den AD-Domänencontroller herunter geladen und im Assistenten hochgeladen werden müssen.

Im ersten Dialog der Einrichtungsassistenten muss der Punkt *Synchronisation von Kontendaten zwischen einer AD und dieser UCS-Domäne* ausgewählt und mit *Weiter* bestätigt werden.

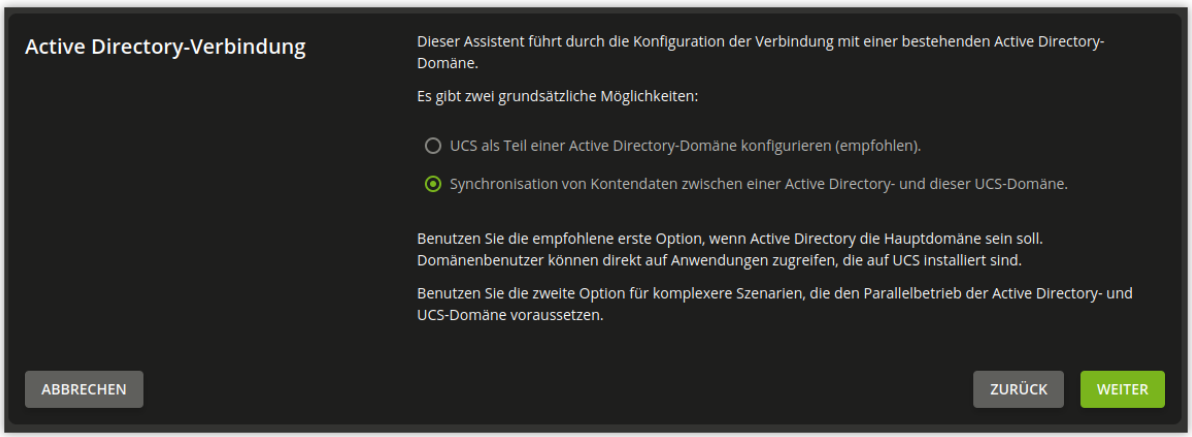


Abb. 9.7: Konfiguration des UCS AD-Connectors über UMC-Modul

Im nächsten Dialog wird die Adresse eines AD-Domänencontrollers abgefragt. Hier kann die IP-Adresse oder ein voll qualifizierter DNS-Name eingegeben werden. Wenn der Rechnername des AD-Systems für das UCS-System nicht auflösbar sein sollte, kann entweder unter UCS der AD DNS-Server als DNS-Forwarder konfiguriert werden oder es kann im UMC-Modul *DNS* ein DNS-Host-Record für das AD-System angelegt werden (siehe *A/AAAA-Records (Host Records)* (Seite 225)).

Alternativ kann auch über Univention Configuration Registry ein statischer Eintrag in `/etc/hosts` aufgenommen werden, z.B. mit

```
$ ucr set hosts/static/192.0.2.100=w2k8-32.ad.example.com
```

Im Feld *Active Directory-Konto* wird der Benutzer konfiguriert, der für den Zugriff auf das AD verwendet wird. Die Einstellung wird in der Univention Configuration Registry Variable `connector/ad/ldap/binddn` (Seite 303) gespeichert. Der Replikationsbenutzer muss im AD Mitglied der Gruppe `Domänen-Admins` sein.

Das verwendete Passwort für den Zugriff muss im Feld *Active Directory-Passwort* eingetragen werden. Es wird auf dem UCS-System lokal in einer Datei gespeichert, die nur für den Benutzer `root` lesbar ist.

Änderung des AD-Zugriffspassworts (Seite 195) beschreibt die Schritte, die notwendig sind, falls diese Zugangsdaten zu einem späteren Zeitpunkt angepasst werden müssen.

Nach Klick auf *Weiter* prüft der Einrichtungsassistent die Verbindung zum AD-Domänencontroller. Falls keine SSL/TLS-verschlüsselte Verbindung aufgebaut werden kann, wird eine Warnung ausgegeben, in der zur Installation einer Zertifizierungsstelle auf dem AD-Domänencontroller geraten wird. Es wird empfohlen diesem Rat zu folgen.

UCS 5.0 erfordert TLS 1.2, welches für Windows Server Releases vor 2012R2 manuell auf dem Windows Server aktiviert werden muss. UCS 5.0 unterstützt die Hash-Funktion SHA-1 nicht mehr. Falls für die Erstellung des AD Root-Zertifikat oder des Zertifikat des Windows Servers dieses Verfahren verwendet wurde, dann sollten diese ersetzt werden.

Nach diesem Schritt kann die Einrichtung durch erneuten Klick auf *Weiter* fortgesetzt werden. Falls weiterhin keine SSL/TLS-verschlüsselte Verbindung aufgebaut werden kann, wird in einem Sicherheitshinweis nachgefragt, ob die Synchronisation ohne SSL-Verschlüsselung eingerichtet werden soll. Falls dies gewünscht ist, kann die Einrichtung durch Klick auf *Fortfahren ohne Verschlüsselung* fortgesetzt werden. In diesem Fall findet die Synchronisation der Verzeichnisdaten unverschlüsselt statt.

Falls der AD-Domänencontroller SSL/TLS-verschlüsselte Verbindungen unterstützt, bietet der Einrichtungsassistent im nächsten Schritt das *Hochladen des AD-Root-Zertifikats* an. Dieses Zertifikat muss vorher aus der AD-Zertifizierungsstelle exportiert werden (siehe *Import des SSL-Zertifikats des Active Directory* (Seite 194)). Falls dieser Schritt hingegen übersprungen wird, kann das Zertifikat auch zu einem späteren Zeitpunkt über das UMC-Modul hochgeladen und die SSL/TLS-Verschlüsselung aktiviert werden (bis dahin werden dann aber alle Verzeichnisdaten unverschlüsselt synchronisiert).

Der Connector kann in verschiedenen Modi betrieben werden, die im nächsten Dialog *Konfiguration der Active Directory-Domänensynchronisation* ausgewählt werden können. Neben einer bidirektionalen Synchronisation kann auch unidirektional von AD nach UCS oder unidirektional von UCS in das AD repliziert werden. Nach Auswahl des Modus muss auf *Weiter* geklickt werden.

Nach einem Klick auf *Weiter* wird die Konfiguration übernommen und der UCS AD-Connector wird gestartet. Der abschließende Dialog muss dann durch Klick auf *Fertigstellen* geschlossen werden.

Nach dieser Einrichtung kann das UMC-Modul *Active Directory-Verbindung* zur weiteren Administration des UCS Active Directory Connectors verwendet werden, z.B. um zu prüfen, ob der Dienst läuft und ihn gegebenenfalls neu zu starten (siehe *Start/Stopp des Active Directory Connectors* (Seite 195)).

Bemerkung: Der Connector kann auch mehrere AD-Domänen mit einer UCS-Domäne synchronisieren; dies ist in *Extended Windows integration documentation* [7] dokumentiert.

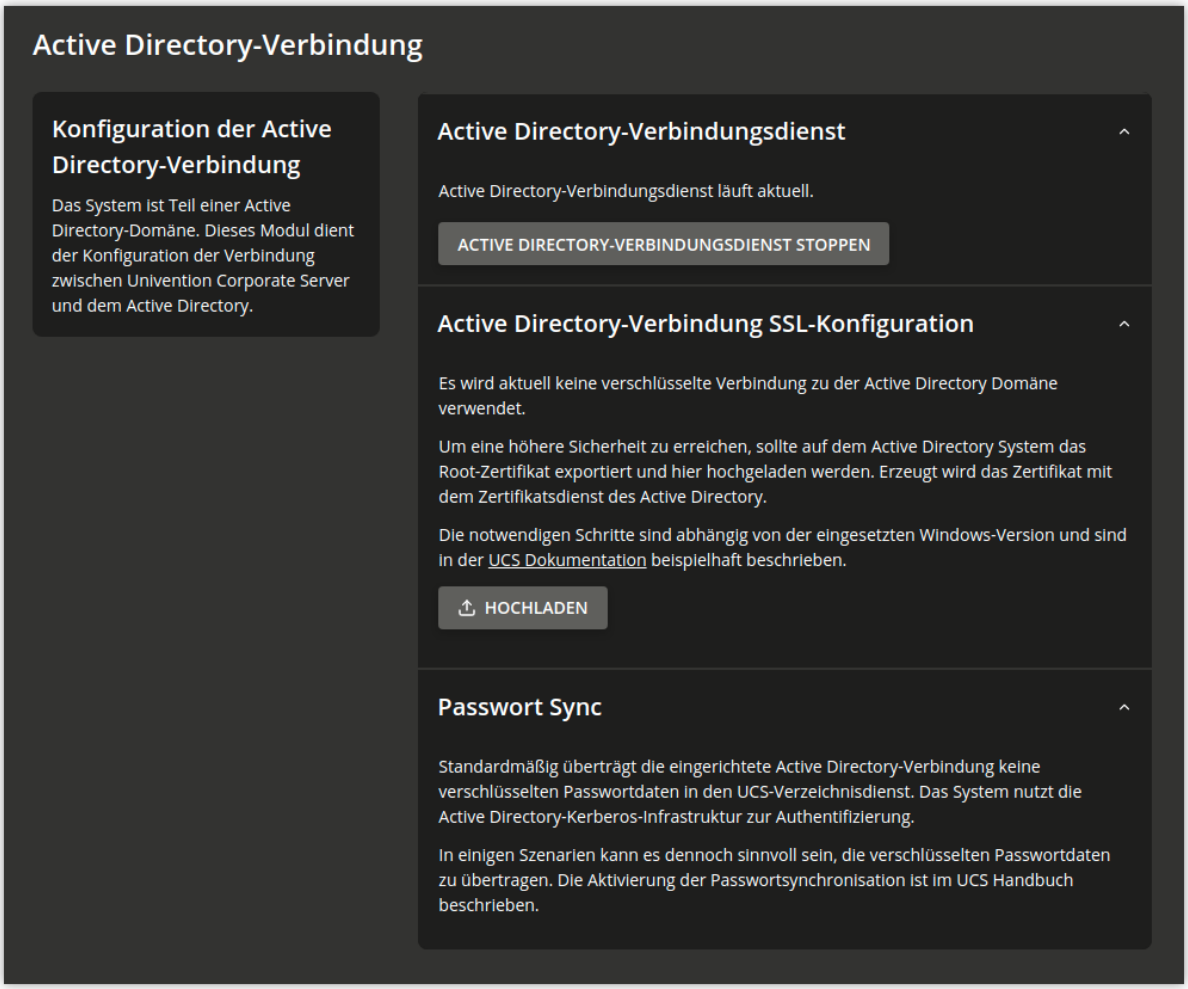


Abb. 9.8: Administrationsdialog für die Active Directory-Verbindung

Import des SSL-Zertifikats des Active Directory

Auf dem Active Directory-System muss nun ein SSL-Zertifikat erzeugt und das Root-Zertifikat exportiert werden, damit eine verschlüsselte Kommunikation stattfinden kann. Erzeugt wird das Zertifikat mit dem Zertifikatsdienst des Active Directory. Die nötigen Schritte sind abhängig von der eingesetzten Windows-Version und werden hier beispielhaft für drei Varianten dargestellt.

Die verschlüsselte Verbindung zwischen UCS-System und Active Directory kann auch deaktiviert werden, indem die Univention Configuration Registry Variable `connector/ad/ldap/ssl` (Seite 304) auf `no` gesetzt wird. Diese Einstellung betrifft nicht die Synchronisation der verschlüsselten Passwortdaten.

Export unter Microsoft Windows Server

Falls der Zertifizierungsdienst noch nicht installiert ist, installieren Sie ihn in Ihre Domäne mit den folgenden Schritten, bevor sie fortfahren:

1. Öffnen Sie den *Server Manager*.
2. Wählen Sie unter *Verwalten* ‣ *Rollen und Features hinzufügen* die Rolle *Active Directory-Zertifikatsdienste* aus.
3. Wählen Sie in der Liste der Dienste die *Zertifizierungsstelle* aus. Die obere Leiste des *Server Manager*s zeigt ein gelbes Warndreieck an.
4. Wählen Sie die Option *Active Directory-Zertifikatsdienste konfigurieren* auf dem Server und konfigurieren Sie die *Zertifizierungsstelle* als ausgewählten Rollendienst.
5. Wählen Sie *Unternehmenszertifizierungsstelle* ‣ *Stammzertifizierungsstelle* als Installationstyp.
6. Klicken Sie *Neuen privaten Schlüssel erstellen*, bestätigen Sie die vorgeschlagenen Verschlüsselungseinstellungen und den Namen der Zertifizierungsstelle.
7. Wählen Sie einen beliebigen Zeitraum für die Gültigkeit und verwenden Sie die Standardpfade für den Speicherort der Datenbank.
8. Starten Sie abschließend Ihren Windows Active Directory Server neu, damit die Änderungen wirksam werden.

Siehe auch:

Installieren der Zertifizierungsstelle[Seite 194, 41]
für eine detaillierte Beschreibung der Installation der Zertifizierungsstelle in *Installieren der Zertifizierungsstelle* [12].

Um das Zertifikat der Zertifizierungsstelle zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie den *Server Manager*.
2. Wählen Sie die Rolle *AD-Zertifikatsdienste*.
3. Klicken Sie mit der rechten Maustaste auf den Namen des Windows-Servers und wählen Sie *Zertifizierungsstelle*. Das Fenster mit der Zertifizierungsstelle öffnet sich. Ein Baum von Rechnern erscheint unter *Zertifizierungsstelle* auf der linken Seite.

   Unter jedem aufgelisteten Rechner befinden sich die Elemente *Gesperrte Zertifikate*, *Ausgestellte Zertifikate*, *Ausstehende Anforderungen*, *Fehlgeschlagene Anforderungen* und *Zertifikatsvorlagen*.
4. Klicken Sie in der Serverliste mit der rechten Maustaste auf den Windows-Server, der Ihre Zertifizierungsstelle bedient, und wählen Sie *Eigenschaften*. Verwechseln Sie ihn nicht mit einem der anderen Elemente.
5. Im Fenster *Eigenschaften* wählen Sie *Generell* ‣ *Stammzertifikat* ‣ *Zertifikat Nr. 0* und klicken auf *Zertifikat anzeigen*.

Wichtig: Es ist wichtig, das Zertifikat zu kopieren, das normalerweise den Namen `Zertifikat Nr. 0` trägt, da die App **`AD Connection`** genau dieses Zertifikat für eine sichere Verbindung benötigt.

---

[41] https://learn.microsoft.com/de-de/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

6. Wählen Sie im sich öffnenden Fenster *Zertifikat* die Registerkarte *Details* und klicken Sie auf *In Datei kopieren* ....

Kopieren des AD-Zertifikats auf das UCS-System

Nun muss das SSL-AD-Zertifikat über das UMC-Modul in das UCS-System importiert werden.

Dies erfolgt durch einen Klick auf *Hochladen* im Untermenü *Active Directory-Verbindung SSL-Konfiguration*. Hierbei öffnet sich ein Fenster, in dem eine Datei ausgewählt wird. Das hochgeladene Zertifikat wird dadurch für den UCS AD-Connector verfügbar gemacht.

Start/Stopp des Active Directory Connectors

Abschließend kann der Connector über *Active Directory-Verbindungsdienst starten* gestartet werden und bei Bedarf über *Active Directory-Verbindungsdienst stoppen* angehalten werden. Alternativ kann ein Starten/Stoppen auch über Kommandozeile durch die Befehle **`/etc/init.d/univention-ad-connector start`** und **`/etc/init.d/univention-ad-connector stop`** erfolgen.

Funktionstest der Grundeinstellungen

Die korrekte Grundkonfiguration des Connectors lässt sich prüfen, indem vom UCS-System aus im Active Directory gesucht wird. Mit folgendem Befehl kann z.B. nach dem Administrator-Konto im Active Directory gesucht werden:

```
$ univention-adsearch cn=Administrator
```

Da **`univention-adsearch`** auf die in Univention Configuration Registry Variable gespeicherte Konfiguration zugreift, kann auf diesem Weg die Erreichbarkeit/Konfiguration des Active Directory-Zugriffs geprüft werden.

Änderung des AD-Zugriffspasswords

Die vom UCS AD-Connector benötigten Zugangsdaten zum Active Directory werden über die Univention Configuration Registry Variable *connector/ad/ldap/binddn* (Seite 303) und *connector/ad/ldap/bindpw* (Seite 303) konfiguriert. Falls das Passwort sich geändert hat oder ein anderes Benutzerkonto verwendet werden soll, können diese Variablen manuell angepasst werden.

Über die Univention Configuration Registry Variable *connector/ad/ldap/binddn* (Seite 303) wird die LDAP-DN eines privilegierten Replikationsbenutzers konfiguriert. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Passwort muss lokal auf dem UCS-System in eine Datei gespeichert werden, deren Dateiname in der Univention Configuration Registry Variable *connector/ad/ldap/bindpw* (Seite 303) eingetragen sein muss. Die Zugriffsrechte für die Datei sollten so eingeschränkt werden, dass nur der Besitzer `root` Zugriff hat. Die folgenden Kommandos zeigen dies beispielhaft:

```
$ eval "$(ucr shell)"
$ echo "Updating ${connector_ad_ldap_bindpw?}"
$ echo "for AD sync user ${connector_ad_ldap_binddn?}"
$ touch "${connector_ad_ldap_bindpw?}"
$ chmod 600 "${connector_ad_ldap_bindpw?}"
$ echo -n "Current AD Syncuser password" > "${connector_ad_ldap_bindpw?}"
```

9.2.4 Werkzeuge / Fehlersuche

Die **Active Directory Connection** stellt die folgenden Werkzeuge und Protokolldateien für die Diagnose zur Verfügung:

univention-adsearch
: Dieses Tool ermöglicht die einfache LDAP-Suche im Active Directory. In AD gelöschte Objekte werden immer mit angezeigt (diese werden in AD weiterhin in einem LDAP-Unterbaum vorgehalten). Als erste Option erwartet das Skript einen LDAP-Filter, die zweite Option kann eine Liste der anzuzeigenden LDAP-Attribute sein, z.B.:

  Beispiel:

```
$ univention-adsearch cn=administrator cn givenName
```

univention-adconnector-list-rejected
: Dieses Tool führt die DNs nicht synchronisierter Objekte auf. Zusätzlich wird, sofern zwischengespeichert, die korrespondierende DN im jeweils anderen LDAP-Verzeichnis angegeben. Abschließend gibt `lastUSN` die ID der letzten von AD synchronisierten Änderung an.

  Dieses Skript könnte eine Fehlermeldung oder eine unvollständige Ausgabe anzeigen, wenn der AD Connector in Betrieb ist.

remove_ad_rejected.py
: Sie können dieses Skript verwenden, um ein AD-Objekt aus der Liste der abgelehnten AD-Objekte zu entfernen, das sich in der internen Datenbankdatei `/etc/univention/connector/internal.sqlite` befindet.

  Beispiel:

```
$ /usr/share/univention-ad-connector/remove_ad_rejected.py \
   -c connector <AD object DN>
```

remove_ucs_rejected.py
: Mit diesem Skript können Sie ein UCS Verzeichnisobjekt aus der Liste der abgelehnten UCS-Objekte entfernen, das sich in der internen Datenbankdatei `/etc/univention/connector/internal.sqlite` befindet.

  Beispiel:

```
$ /usr/share/univention-ad-connector/remove_ucs_rejected.py \
   -c connector <UCS object DN>
```

resync_object_from_ad.py
: Sie können dieses Skript verwenden, um Verzeichnisobjekte von AD zu UCS erneut zu synchronisieren. Verwenden Sie es, um ein einzelnes oder mehrere Verzeichnisobjekte zu synchronisieren.

  Beispiel:

```
# to re-sychronize a single object
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \
    -c connector <object DN>

# to re-synchronize all objects matching a specific filter
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \
    -c connector \
    --filter "(objectClass=posixAccount)"

# to re-synchronize all objects matching a specific base
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \
    -c connector \
    --filter "(objectClass=posixAccount)" \
    --base "dc=example,dc=com"
```

resync_object_from_ucs.py
Sie können dieses Skript verwenden, um Verzeichnisobjekte von UCS nach AD erneut zu synchronisieren. Verwenden Sie es, um ein einzelnes oder mehrere Verzeichnisobjekte zu synchronisieren.

Beispiele:

```
# to re-synchronize a single object
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \
   -c connector <object DN>

# to re-synchronize all objects matching a specific filter
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \
   -c connector \
   --filter "<LDAP filter>" \

# to re-synchronize all objects matching a specific base
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \
   -c connector \
   --filter "<LDAP filter>" \
   --base "<base dn>" \
```

prepare-new-instance
Sie können dieses Skript verwenden, um AD-Verbindungsinstanzen zu erstellen. Das Skript kopiert die erforderlichen Dateien und setzt bestimmte UCR-Variablen.

Alternativ können Sie dieses Skript auch verwenden, um eine AD-Verbindungsinstanz zu löschen. Das Skript löscht dann intern die Dateien für die Instanz und setzt die UCR-Variablen zurück.

well-known-sid-object-rename
Sie können dieses Skript verwenden, um Benutzer und Gruppen mit bekannten SIDs in UDM umzubenennen. Die **AD Connection** verwendet es, um Benutzer und Gruppen mit bekannten SIDs umzubenennen.

make-deleted-objects-readable-for-this-machine
Sie können dieses Skript verwenden, um Zugriff zum Auflisten und Lesen auf `CN=Deleted Objects` in Active Directory zu gewähren.

Logdateien
Zur Fehlersuche bei Synchronisationsproblemen finden sich entsprechende Meldungen in folgenden Dateien auf dem UCS-System:

- `/var/log/univention/connector-ad.log`
- `/var/log/univention/connector-ad-status.log`

9.2.5 Selektive Synchronisation

Sie können die **Active Directory Connection** so konfigurieren, dass nur eine bestimmte Auswahl von Quellobjekten synchronisiert wird. Sie können die Quellobjekte nach Kriterien auswählen, die in den folgenden Abschnitten ausführlich beschrieben werden:

- Auswahl von Objekten nach Standort im LDAP-Teilbaum
- Auswahl von Objekten durch Übereinstimmung mit einem LDAP-Filter
- Auswahl aller Elemente außer nach Standort im LDAP-Teilbaum
- Auswahl aller Elemente außer durch Übereinstimmung mit einem LDAP-Filter

Nur bestimmte LDAP-Teilbäume zulassen

Um den Connector so zu konfigurieren, dass er nur bestimmte Teilbäume der LDAP-Struktur synchronisiert, können Sie die folgenden UCR-Variablen verwenden:

connector/ad/mapping/allowsubtree/.*/ucs

Für die Synchronisation von UCS LDAP-Verzeichnis zu Active Directory

Verwenden Sie diese Univention Configuration Registry Variable, um einen DN aus Ihrem UCS LDAP-Verzeichnis für die Synchronisation mit dem angeschlossenen Active Directory zu definieren. Die *AD-Verbindung* berücksichtigt dann nur UCS LDAP-Objekte für die Synchronisation, die sich in Teilbäumen befinden, die durch eine dieser UCR-Variablen spezifiziert sind. Die LDAP-Basis muss in den DNs enthalten sein und der Vergleich der DNs ist unabhängig von der Groß- und Kleinschreibung.

Siehe die Erklärung des Platzhalters `.*` weiter unten.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/allowsubtree/school1/ucs="ou=school1,dc=ucs,
↪domain"
$ ucr set connector/ad/mapping/allowsubtree/school2/ucs="ou=school2,dc=ucs,
↪domain"
```

connector/ad/mapping/allowsubtree/.*/ad

Für die Synchronisation von Active Directory zum UCS Verzeichnisdienst

Verwenden Sie diese Univention Configuration Registry Variable, um einen DN aus Ihrem Active Directory für die Synchronisation mit Ihrem UCS LDAP-Verzeichnis zu definieren. Die *AD-Verbindung* berücksichtigt dann nur Active Directory Objekte für die Synchronisation, die sich in Teilbäumen befinden, die durch eine dieser UCR-Variablen festgelegt sind. Die LDAP-Basis muss in den DNs enthalten sein, und beim Vergleich der DNs wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Siehe die Erklärung des Platzhalters `.*` weiter unten.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/allowsubtree/school1/ad="ou=school1,dc=ad,domain
↪"
$ ucr set connector/ad/mapping/allowsubtree/school2/ad="ou=school2,dc=ad,domain
↪"
```

Platzhalter .*

Der Teil `.*` der Variable ist ein Platzhalter, den Sie als individuelle Bezeichnung für jede Variable verwenden können. Wenn Sie diesen Ansatz verfolgen, können Sie eine Reihe von UCR-Variablen der beschriebenen Typen erstellen. Jede Variable enthält nur einen DN.

Für jeden LDAP-Teilbaum, den Sie für die Synchronisierung zulassen möchten, müssen Sie eine separate Univention Configuration Registry Variable konfigurieren.

Nachdem Sie die UCR-Variablen definiert oder geändert haben, müssen Sie die **Active Directory Verbindung** neu starten.

Tipp: Die **Active Directory Verbindung** bestimmt die Position des Zielobjekts durch dynamische und statische Faktoren wie die Mapping Attribute `dn_mapping_function` und `position_mapping`, sofern sie im Mapping für einzelne Objekttypen konfiguriert sind. Die Position des entsprechenden Zielobjekts kann also außerhalb der Teilbäume liegen, die den Univention Configuration Registry Variablen entsprechen.

Warnung: Wenn Sie die Konfiguration …`/allowsubtree/.*/[ad|ucs]` verwenden und ein Quellobjekt aus einem betrachteten Teilbaum an eine Position verschieben, die außerhalb des kombinierten Geltungsbereichs

aller Ihrer …/allowsubtree/.*/[ad|ucs] Definitionen liegt, dann entfernt die **Active Directory Verbindung** das Objekt aus dem Zielverzeichnis.

Nur Objekte zulassen, die einem LDAP-Filter entsprechen

Sie können für jede Art von Objekt einen LDAP-Filter konfigurieren. **Active Directory Verbindung** synchronisiert nur LDAP-Objekte, die diesem Filter entsprechen. Alle anderen LDAP-Objekte werden ignoriert.

Für die bidirektionale Synchronisierung muss der Filter sowohl mit dem UCS Objekt als auch mit dem AD-Objekt übereinstimmen. Wird ein Objekt, das mit dem Filter übereinstimmt, gelöscht, löscht der Connector auch das entsprechende Objekt auf der anderen Seite.

connector/ad/mapping/{type}/allowfilter

Der Connector synchronisiert nur die Objekte mit dem Objekttyp {type}, die diesem LDAP-Filter entsprechen. {type} kann einer der folgenden Werte sein:

- user
- group
- container
- ou
- windowscomputer

Zum Beispiel:

```
$ ucr set connector/ad/mapping/user/allowfilter="(description=sync)"
```

Nach dem Ändern dieser Einstellungen müssen Sie die **Active Directory Verbindung** neu starten.

Bemerkung: Dieser Filter unterstützt jedoch nicht die vollständige LDAP-Filtersyntax. Es wird immer zwischen Groß- und Kleinschreibung unterschieden. Sie können nur den Platzhalter * als Einzelwert ohne andere Zeichen verwenden.

Wichtig: Wenn ein Objekt, das mit dem Filter übereinstimmt, so geändert wird, dass der Filter nicht mehr passt, **synchronisiert** der Connector keine Änderung. Das bedeutet, dass der Connector weiterhin Änderungen von der anderen Seite auf das Objekt anwendet.

Wenn Sie die Synchronisierung für ein Objekt ausschalten wollen, müssen Sie die Änderung auf beiden Seiten, UCS und Active Directory, vornehmen.

Ignorieren von Objekten aus bestimmten LDAP-Teilbäumen

Um den Connector so zu konfigurieren, dass er Objekte aus bestimmten LDAP-Teilbäumen ignoriert, können Sie die folgende Univention Configuration Registry Variable verwenden:

connector/ad/mapping/ignoresubtree/.*

Die Variable definiert die Stellen im Verzeichnisdienst, die der Connector von der Synchronisation ausschließt. Die Werte können Positionen in Active Directory und im UCS LDAP-Verzeichnis enthalten. Standardmäßig ist die Variable nicht gesetzt.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/ignoresubtree/ignore1="cn=alumni,dc=ucs,domain"
$ ucr set connector/ad/mapping/ignoresubtree/ignore2="cn=alumni,dc=ad,domain"
```

Nach der Änderung dieser Einstellung müssen Sie die **Active Directory Verbindung** neu starten.

Objekte durch LDAP-Filter ignorieren

Um Objekte von der Synchronisierung auszuschließen, können Sie ihre Namen zu den folgenden Univention Configuration Registry Variable hinzufügen:

connector/ad/mapping/{type}/ignorelist

Der Connector synchronisiert **keine** Objekte, die diese Variable als Werte definiert. Trennen Sie mehrere Werte durch Kommas. Für die möglichen Werte für `{type}`, siehe Tab. 9.1. Die Tabelle zeigt auch, welche LDAP-Attribute Sie je nach Objekttyp im Filter berücksichtigen müssen.

Tab. 9.1: Zuordnung, welcher `{type}` welches LDAP-Attribut benötigt

{type}	Wert aus LDAP-Attribut
user	uid
group	cn
container	cn
ou	ou
windowscomputer	cn

Der Typ `user` berücksichtigt zum Beispiel das LDAP-Attribut `uid`:

```
$ ucr set connector/ad/mapping/user/ignorelist="Administrator,krbtgt,root,
↪pcpatch,mmustermann"
```

Wichtig: Einige der `ignorelist`-Einstellungen haben Voreinstellungen, die für die Funktionalität des Connector wichtig sind. Achten Sie darauf, dass Sie diese Einstellungen nicht überschreiben. Sie können den aktuellen Wert einer Univention Configuration Registry Variable mit dem folgenden Befehl überprüfen:

```
$ ucr get connector/ad/mapping/user/ignorelist
```

Für mehr Flexibilität können Sie auch einen LDAP-Filter setzen, um Objekte zu ignorieren. Verwenden Sie die folgende Univention Configuration Registry Variable:

connector/ad/mapping/{type}/ignorefilter

Der Connector synchronisiert **keine** Objekte, die diesem LDAP-Filter entsprechen. `{type}` kann einen der folgenden Werte haben:

- `user`
- `group`
- `container`
- `ou`
- `windowscomputer`

Zum Beispiel:

```
$ ucr set connector/ad/mapping/user/ignorefilter="(description=no sync)"
```

Bemerkung: Dieser Filter unterstützt jedoch nicht die vollständige LDAP-Filtersyntax. Es wird immer zwischen Groß- und Kleinschreibung unterschieden. Sie können nur den Platzhalter `*` als Einzelwert ohne andere Zeichen verwenden.

Nach dem Ändern dieser Einstellungen müssen Sie die **Active Directory Verbindung** neu starten.

Vorrang der Regeln

In diesem Abschnitt wird die Verarbeitungsreihenfolge für die bisher dokumentierten Einstellungen zur selektiven Synchronisation beschrieben.

Die **`Active Directory Verbindung`** verarbeitet die Regeln für Erlauben und Ignorieren in einer definierten Reihenfolge. Abhängig vom Ergebnis der Auswertung verhält sich der Connector wie folgt:

- Wenn eine Regel dazu führt, dass der Connector ein Objekt ignoriert, stoppt der Connector die Verarbeitung der Regel und synchronisiert kein Objekt.
- Wenn eine Regel dazu führt, dass der Connector ein Objekt verarbeitet, wertet der Connector die nächste Regel aus. Wenn die Regel die letzte Regel war und es keine nächste Regel gibt, synchronisiert der Connector das Objekt.

Der Connector wertet die Regeln für jedes Objekt in der folgenden Reihenfolge aus:

1. **Teilbaum zulassen**:

   UCR Variablen
   connector/ad/mapping/allowsubtree/./ucs* (Seite 198) und *connector/ad/mapping/allowsubtree/.*/ad* (Seite 198)

   Keine Übereinstimmung
   Keine Synchronisation. Abarbeitung der Regeln beenden.

   Übereinstimmung
   Fortsetzen.

2. **Filter zulassen**:

   UCR Variable
   connector/ad/mapping/{type}/allowfilter (Seite 199)

   Keine Übereinstimmung
   Keine Synchronisation. Abarbeitung der Regeln beenden.

   Übereinstimmung
   Fortsetzen.

3. **Unterbaum ignorieren**:

   UCR Variable
   *connector/ad/mapping/ignoresubtree/.** (Seite 199)

   Keine Übereinstimmung
   Fortsetzen.

   Übereinstimmung
   Keine Synchronisation. Abarbeitung der Regeln beenden.

4. **Filter ignorieren**:

   UCR Variablen
   connector/ad/mapping/{type}/ignorelist (Seite 200) und *connector/ad/mapping/{type}/ignorefilter* (Seite 200)

   Keine Übereinstimmung
   Fortsetzen.

   Übereinstimmung
   Keine Synchronisation. Abarbeitung der Regeln beenden.

5. **Ende der Regeln**.

6. **Objekt synchronisieren**.

9.2.6 Details zur vorkonfigurierten Synchronisation

Standardmäßig schließt die **Active Directory Verbindung** einige LDAP-Teilbäume von der Synchronisation aus. Sie finden die Liste der ignorierten Teilbäume in der Datei `/var/log/univention/connector-ad-mapping.log` unter der Einstellung `ignore_subtree` für jeden Objekttyp.

Container und Organisationseinheiten

Container und Organisationseinheiten werden zusammen mit ihrer Beschreibung synchronisiert. Die Container `cn=mail` und `cn=kerberos` werden auf beiden Seiten ignoriert. Bei Containern sind einige Besonderheiten auf AD-Seite zu beachten. Active Directory bietet im *Manager für Benutzer und Gruppen* keine Möglichkeit, Container anzulegen. AD zeigt diese im erweiterten Modus aber an (*Ansicht ▸ Erweiterte Funktionen*).

Berücksichtigen Sie die folgenden Besonderheiten:

- Unter AD gelöschte Container oder Organisationseinheiten werden unter UCS rekursiv gelöscht, das bedeutet, dass nicht synchronisierte Unterobjekte, die in AD nicht zu sehen sind, ebenfalls entfernt werden.

Gruppen

Gruppen werden anhand des Gruppennamens synchronisiert, dabei findet eine Berücksichtigung der primären Gruppe eines Benutzers statt (die unter AD nur am Benutzer im LDAP hinterlegt wird).

Gruppenmitglieder, die im anderen System z.B. aufgrund von Ignore-Filtern kein Gegenstück haben, werden ignoriert (bleiben also Mitglied der Gruppe).

Zusätzlich wird die Beschreibung der Gruppe synchronisiert.

Besonderheiten

Berücksichtigen Sie die folgenden Besonderheiten:

- Unter AD wird der *Prä-Windows 2000 Name* (LDAP-Attribut `samAccountName`) verwendet, daher kann eine Gruppe im Active Directory mit anderem Namen erscheinen als unter UCS.
- Der Connector ignoriert Gruppen, die im Univention Directory Manager unter *Samba Gruppentyp* als *Bekannte Gruppe* konfiguriert wurden. Eine Synchronisation von SID oder RID findet nicht statt.
- Gruppen, die im Univention Directory Manager unter *Samba Gruppentyp* als *Lokale Gruppe* konfiguriert wurden, werden vom Connector als *globale Gruppen* in das Active Directory synchronisiert.
- Neu angelegte oder verschobene Gruppen werden immer im gleichen Untercontainer auf der Gegenseite angelegt. Existieren während der Initialisierung gleichnamige Gruppen in unterschiedlichen Containern, werden die Mitglieder synchronisiert, nicht jedoch die Position im LDAP. Wird eine solche Gruppe auf einer Seite verschoben ist der Zielcontainer auf der anderen Seite identisch, so dass sich die DNs der Gruppen ab diesem Zeitpunkt nicht mehr unterscheiden.
- Bestimmte Gruppennamen werden anhand einer Mapping-Tabelle umgesetzt, so dass z.B. die UCS-Gruppe `Domain Users` mit der AD-Gruppe `Domänen-Benutzer`. synchronisiert wird. Dieses Mapping kann in englischsprachigen AD-Domänen dazu führen, das die deutschsprachigen Gruppen angelegt werden und sollte in diesem Fall deaktiviert werden. Dazu kann die Univention Configuration Registry Variable *`connector/ad/mapping/group/language`* (Seite 304) verwendet werden.

  Die vollständige Tabelle ist:

UCS-Gruppe	*AD-Gruppe*
`Domain Users`	`Domänen-Benutzer`
`Domain Admins`	`Domänen-Admins`
`Windows Hosts`	`Domänencomputer`

- Die Repräsentation von Gruppen in Gruppen unterscheidet sich zwischen AD und UCS. Sind unter UCS Gruppen Mitglieder von Gruppen, so können diese Objekte nicht immer auf AD-Seite synchronisiert werden und erscheinen in der Liste der zurückgewiesenen Objekte. Verschachtelte Gruppen sollten daher aufgrund der in Active Directory vorliegenden Einschränkungen immer nur dort zugewiesen werden.
- Wird im Univention Directory Manager eine globale Gruppe `A` als Mitglied einer anderen globalen Gruppe `B` aufgenommen, so erscheint diese Mitgliedschaft aufgrund von AD-internen Beschränkungen unter **`Windows 2000/2003`** nicht im Active Directory. Wird Gruppe `A` anschließend umbenannt, geht die Gruppenmitgliedschaft in Gruppe `B` verloren. Ab **`Windows 2008`** besteht diese Einschränkung nicht mehr, dort können im Active Directory auch globale Gruppen verschachtelt werden.

Benutzerdefinierte Mappings

Für benutzerdefinierte Mappings, siehe Active Directory Connection custom mappings[42] in *Univention Developer Reference* [3].

Benutzer

Benutzer werden wie Gruppen anhand des Benutzernamens und anhand des AD-Windows 2000 Namens synchronisiert. Direkt übermittelt werden die Attribute *Vorname*, *Nachname*, *primäre Gruppe* (sofern auf der anderen Seite vorhanden), *Organisation*, *Beschreibung*, *Straße*, *Stadt*, *PLZ*, *Profilpfad*, *Anmeldeskriptpfad*, *Deaktiviert* und *Kontoablaufdatum*. Indirekt werden zusätzlich *Passwort*, *Passwortablaufdatum* und *Ändern des Passwortes beim nächsten Login* synchronisiert. Vorbereitet, aber auf Grund unterschiedlicher Syntax in der Mapping-Konfiguration auskommentiert, sind *Primäre Mail-Adresse* und *Telefonnummer*.

Ausgenommen werden die Benutzer `root` und `Administrator`.

Berücksichtigen Sie die folgenden Besonderheiten:

- Benutzer werden ebenfalls anhand des Namens identifiziert, so dass für Benutzer, die vor der ersten Synchronisation auf beiden Seiten angelegt wurden, hinsichtlich der Position im LDAP das gleiche Verhalten gilt wie bei Gruppen.
- Es kann vorkommen, dass ein unter AD anzulegender Benutzer, dessen Passwort zurückgewiesen wurde, nach sofortigem erneuten Anlegen aus AD gelöscht wird. Grund dafür ist, das AD diesen Benutzer zunächst anlegt und nach dem Abweisen des Passwortes sofort wieder löscht. Werden diese Operationen nach UCS übertragen, werden sie auch wieder zurück nach AD übermittelt. Wurde der Benutzer auf AD-Seite schon vor der Rückübertragung der Operation erneut eingetragen, so wird er nach der Rückübertragung gelöscht. Das Auftreten dieses Verhaltens ist abhängig von dem eingestellten Abfrageintervall des Connectors.
- AD und UCS legen neue Benutzer per Voreinstellung in eine bestimmte primäre Gruppe (meist `Domain Users` und `Domänen Benutzer`). Während der ersten Synchronisation von UCS nach AD werden die Benutzer daher immer in dieser Gruppe Mitglied.

9.3 Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover

UCS unterstützt die Übernahme von Benutzern, Gruppen, Rechnerobjekten und Gruppenrichtlinienobjekten (GPOs) aus einer bestehenden Active Directory (AD)-Domäne. Die Windows-Clients müssen dabei nicht erneut der Domäne beitreten. Diese Übernahme ist ein interaktiver Prozess, der aus drei Phasen besteht:

1. Kopieren aller Objekte aus Active Directory nach UCS
2. Kopieren der Gruppenrichtliniendateien aus Active Directory nach UCS
3. Abschalten des AD-Servers und Zuweisung der FSMO-Rollen auf den UCS Directory Node

[42] https://docs.software-univention.de/developer-reference/5.0/en/misc.html#ad-connection-custom-mappings

Die folgenden Voraussetzungen müssen für die Übernahme erfüllt sein:

- Der UCS Directory Node (Primary Directory Node) muss mit einem eindeutigen Rechnernamen installiert werden, der nicht in der AD-Domäne vorhanden ist.
- Der UCS Directory Node muss mit demselben DNS-Domänennamen, NetBIOS-Domänennamen und Kerberos-Domänennamen installiert werden wie die AD-Domäne. Es wird empfohlen auch die selbe LDAP-Basis-DN zu verwenden.
- Der UCS Directory Node muss eine IPv4-Adresse im selben Subnetz wie der zu übernehmende Active Directory-Domänencontroller verwenden.

Vorsicht: Sofern das System bereits Mitglied in einer Active Directory Domäne ist, wird durch die Installation der *Active Directory Takeover* Applikation diese Mitgliedschaft entfernt. Deshalb sollte die Installation der *Takeover* Applikation erst kurz vor der eigentlichen Übernahme der Active Directory Domäne erfolgen.

Für die Migration muss die Applikation **`Active Directory Takeover`** aus dem Univention App Center installiert werden. Sie muss auf dem System installiert werden, auf dem der Univention S4 Connector läuft (siehe *Univention S4 Connector* (Seite 179), normalerweise der Primary Directory Node).

9.3.1 Vorbereitung

Es wird empfohlen die folgenden Schritte durchzuführen, bevor die Übernahme initiiert wird:

- Ein Backup des/der AD-Server(s) sollte durchgeführt werden.
- Sind Benutzeranmeldungen auf dem AD-Server erlaubt (durch Domänenanmeldungen oder Terminalserversitzungen), wird empfohlen, diese zu deaktivieren und alle Dienste zu stoppen, die Daten verarbeiten (z.B. Mailserver). Dies stellt sicher das durch den Rollback auf ein Backup oder einen Snapshot keine Daten verloren gehen.
- Es wird empfohlen auf dem AD-Server dasselbe `Administrator`-Passwort zu verwenden wie in der UCS-Domäne. Werden verschiedene Passwörter verwendet, wird anhand der Zeitstempel verglichen, welches Passwort aktueller ist und dieses verwendet.
- In der Grundeinstellung ist das lokale `Administrator` Konto auf dem AD-Server deaktiviert. Es sollte in der lokalen Benutzerverwaltung aktiviert werden.

Die Aktivierung des `Administrator`-Kontos wird empfohlen, weil dieses Konto über die nötigen Berechtigungen verfügt, um die Gruppenrichtlinien-Dateien in der SYSVOL-Freigabe zu kopieren. Der Benutzer kann entweder im AD-Verwaltungs-Tool für Benutzer und Gruppen oder mit den folgenden Kommandos auf der Kommandozeile aktiviert werden:

```
> net user administrator /active:yes
> net user administrator PASSWORD
```

9.3.2 Domänenmigration

Die Übernahme muss auf dem UCS Directory Node gestartet werden, auf dem der Univention S4 Connector läuft (normalerweise der Primary Directory Node). Während der Übernahme sollte Samba nur auf diesem UCS-System laufen. Gibt es weitere UCS Samba/AD Nodes, muss Samba auf diesen angehalten werden. Dies ist wichtig um replikationsbedingte Dateninkonsistenzen zu vermeiden.

Andere UCS Samba/AD-Systeme können gestoppt werden, indem auf jedem UCS Directory Node als Benutzer `root` folgender Befehl ausgeführt wird

```
$ /etc/init.d/samba4 stop
```

Nachdem sichergestellt wurde, dass keine anderen Samba/AD-Domänencontroller laufen, kann die Übernahme beginnen. Wurde die UCS-Domäne mit einer UCS-Version vor 3.2 installiert, muss zuerst die folgende Univention Configuration Registry Variable gesetzt werden:

```
$ ucr set connector/s4/mapping/group/grouptype=false
```

Die Übernahme erfolgt mit dem UMC-Modul *Active Directory Takeover*. Unter *Name oder Adresse des Domänencontrollers* muss die IP-Adresse des AD-Systems angegeben werden. Unter *Active Directory Administratorkonto* muss ein Konto der AD-Domäne angegeben werden, das Mitglied der AD-Gruppe `Domain Admins` ist (z.B. der `Administrator`) und unter *Active Directory Administratorpasswort* das dazugehörige Passwort.

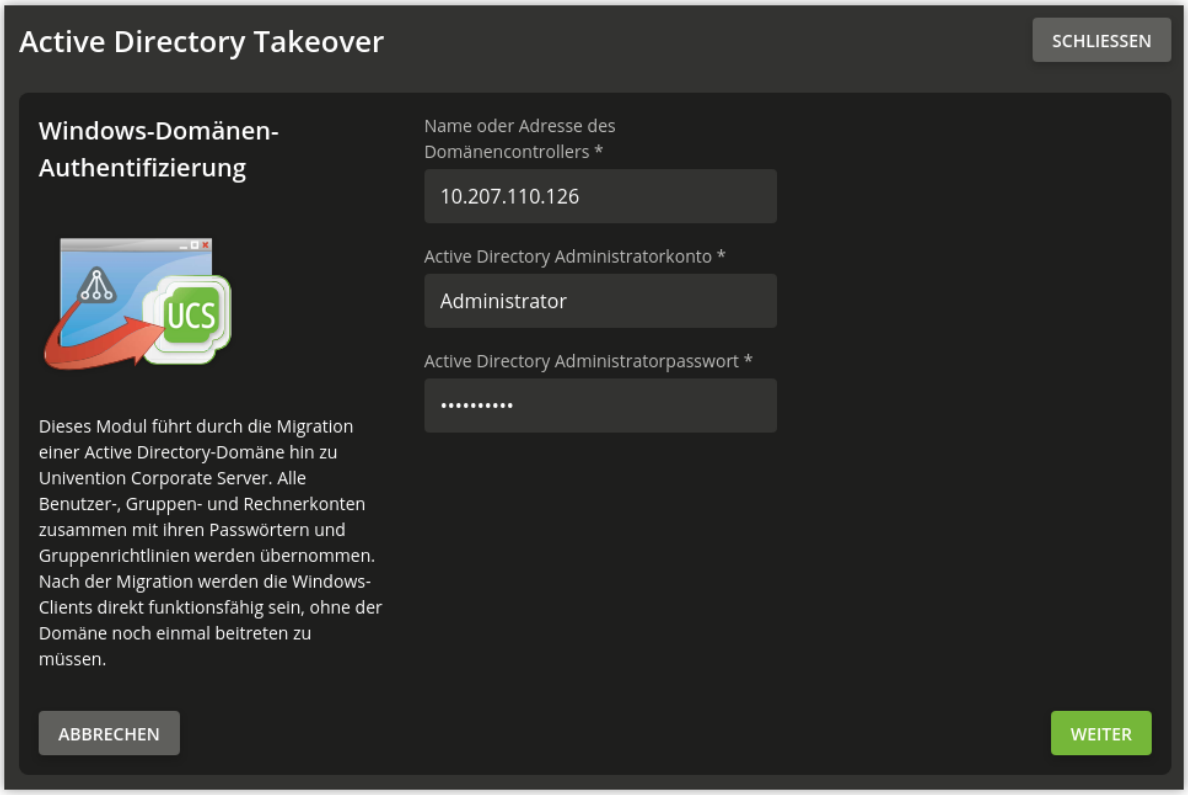


Abb. 9.9: Erste Phase der Domänenmigration

Das Modul prüft, ob der AD-Domänencontroller erreicht werden kann und zeigt die zu migrierenden Domänendaten an.

Nach einem Klick auf *Weiter* werden die folgenden Schritte automatisch durchgeführt:

1. Anpassung der Systemzeit des UCS-Systems auf die Systemzeit der Active Directory-Domäne (wenn diese um mehr als drei Minuten nachgeht).
2. Beitritt des UCS Directory Nodes in die Active Directory-Domäne.
3. Start von Samba und dem Univention S4 Connector zur Replikation der AD-Objekte in das UCS-OpenLDAP-Verzeichnis.
4. Wenn ein Benutzerkonto oder eine Gruppe mit einer „*Well Known*“ RID nach UCS OpenLDAP synchronisiert wird, setzt ein Listener-Modul auf jedem UCS-System lokal eine Univention Configuration Registry Variable, die dem englischen Namen den nicht-englischen Namen zuordnet.

   Diese Variablen werden verwendet, um die in den UCS-Konfigurationsdateien verwendeten englischen Begriffe in die im Active Directory verwendeten Namen zu übersetzen. Wenn zum Beispiel `Domain Admins` einen anderen Namen im AD hat, dann wird die Univention Configuration Registry Variable *groups/default/domainadmins* (Seite 306) auf den spezifischen Namen gesetzt (analog für Benutzer, z.B. *users/default/administrator* (Seite 319)).

Abb. 9.10: Übersicht über die zu migrierenden Daten

Zusätzliche Informationen werden nach `/var/log/univention/ad-takeover.log` sowie nach `/var/log/univention/management-console-module-adtakeover.log` protokolliert.

Nun enthält der UCS Directory Node alle Benutzer, Gruppen und Rechner aus der Active Directory-Domäne. Im nächsten Schritt wird die SYSVOL-Freigabe kopiert, in der u.a. die Gruppenrichtlinien gespeichert werden.

Nun muss eine Anmeldung als `Administrator` am Active Directory-Domänencontroller erfolgen und dort die Dateien mit den Gruppenrichtlinien aus der SYSVOL-Freigabe des AD-Servers auf den UCS-Server kopiert werden.

Das aufzurufende Kommando wird im UMC-Modul angezeigt. Wenn es erfolgreich aufgerufen wurde, muss mit *Weiter* bestätigt werden.

Abb. 9.11: Kopieren der SYSVOL-Freigabe

Wenn **`robocopy`** nicht vorhanden ist, kann es mit den Windows Server 2003 Resource Kit Tools nachinstalliert werden. Ab Windows 2008 ist es vorinstalliert.

Bemerkung: Hinweis: Die **`robocopy`**-Option `/mir` spiegelt das Quellverzeichnis mit dem Zielverzeichnis. Es muss beachtet werden, dass bei einem erneuten Aufruf des Tools Dateien, die im Quellverzeichnis gelöscht wurden, auch im Zielverzeichnis gelöscht werden.

Nach erfolgreichem Abschluss dieser Schritte sollten der/die AD-Domänencontroller heruntergefahren werden. Anschließend muss im UMC-Modul auf *Weiter* geklickt werden.

Abb. 9.12: Herunterfahren des/der AD-Systeme

Die folgenden Schritte werden nun automatisch durchgeführt:

1. Übertragung der FSMO-Rollen auf den UCS Directory Node. Diese kennzeichnen verschiedene Aufgaben, die ein Server in einer AD-Domäne übernehmen kann.
2. Einrichten des Rechnernamens des AD-Servers als DNS-Alias (siehe *CNAME-Record (Alias-Records)* (Seite 225)) für den UCS-Server.
3. Konfiguration der IP-Adresse des AD-Servers als zusätzliche virtuelle IP-Adresse des UCS-Servers.
4. Verschiedene Anpassungen, z.B. Entfernen des alten AD-Domänencontroller-Eintrags aus der Samba SAM-Datenbank.
5. Abschließender Neustart von Samba und DNS-Server.

9.3.3 Abschluss der Übernahme

Abschließend müssen noch die folgenden Schritte durchgeführt werden:

1. Der Domänenfunktionslevel der migrierten AD-Domäne muss mit dem folgenden Kommando geprüft werden:

   ```
   > samba-tool domain level show
   ```

   Wenn das Kommando die Meldung `ATTENTION: You run SAMBA 4 on a forest function level lower than Windows 2000 (Native)` anzeigt, müssen die folgenden Befehle aufgerufen werden:

   ```
   > samba-tool domain level raise --forest-level=2003 --domain-level=2003
   > samba-tool dbcheck --fix --yes
   ```

2. Gab es in der migrierten AD-Domäne mehr als einen Domänencontroller, müssen die Rechnerkonten der weiteren Domänencontroller im UMC-Modul *Rechnerverwaltung* gelöscht werden. Außerdem müssen sie aus der Samba SAM-Datenbank gelöscht werden. Dies kann erreicht werden, indem von einem migrierten Windows-Client eine Anmeldung als Mitglied der Gruppe `Domain Admins` erfolgt und das AD-Verwaltungstool für Benutzer und Computer aufgerufen wird.
3. Gibt es weitere Samba-Domänencontroller, müssen diese neu der Domäne beitreten.
4. Alle Windows-Clients müssen neu gestartet werden.

9.3.4 Tests

Es wird empfohlen nach der Übernahme gründliche Tests mit Windows-Clients durchzuführen, z.B.

- Anmeldung auf einem migrierten Client mit einem migrierten Benutzer.
- Anmeldung auf einem migrierten Client als *Administrator*.
- Test der Gruppenrichtlinien.
- Domänenbeitritt eines neuen Windows-Clients.
- Anlegen eines neuen Benutzers und Anmeldung an einem Windows-Client.

9.4 Vertrauensstellungen

Vertrauensstellungen zwischen Domänen ermöglichen es den Benutzern einer Domäne, sich an Rechnern einer anderen Domäne anzumelden.

Vertrauensstellungen können unidirektional oder bidirektional eingerichtet werden. Technisch entspricht eine bidirektionale Vertrauensstellung zwei unidirektional konfigurierten Vertrauensstellungen in beide Richtungen.

Die Terminologie von Vertrauensstellungen hängt von der Perspektive der vertrauenden oder der vertrauten Domäne ab: Aus Sicht der vertrauenden Domäne ist die Vertrauensstellung *ausgehend* und aus Sicht der vertrauten Domäne *eingehend*.

Ausgehende Vertrauensstellungen (UCS vertraut Windows) werden in Samba/AD-Domänen nicht unterstützt. Entsprechend werden auch keine bidirektionalen Vertrauensstellungen unterstützt.

Während der Einrichtung und Nutzung von Vertrauensstellungen müssen sich die Domänencontroller der beiden Domänen über das Netzwerk erreichen und gegenseitig per DNS identifizieren können. Zumindest die voll qualifizierten DNS Namen der Domänencontroller der jeweils anderen Domäne müssen auflösbar sein, damit die Kommunikation zwischen den Domänen funktioniert. In beiden Domänen richtet man zu diesem Zweck eine bedingte DNS Weiterleitung ein.

Für das folgende Beispiel sei angenommen, dass der UCS Samba/AD DC Primary Directory Node `primary.ucsdom.example` die IP-Adresse `192.0.2.10` hat und dass der Active Directory Domänencontroller `dc1.addom.example` der entfernten Domäne die IP-Adresse `192.0.2.20` hat.

Auf der UCS-Seite lässt sich die bedingte Weiterleitung von DNS-Anfragen mit folgenden Schritten als `root` einrichten:

```
$ cat >>/etc/bind/local.conf.samba4 <<__EOT__
zone "addom.example" {
  type forward;
  forwarders { 192.0.2.20; };
};
__EOT__
$ systemctl restart bind9
```

Der Erfolg kann mit folgendem Befehl überprüft werden:

```
$ host dc1.addom.example
```

Zusätzlich kann es sinnvoll sein, für den Domänencontroller der entfernten Active Directory Domäne einen statischen Eintrag in der Datei `/etc/hosts` anzulegen:

```
$ ucr set hosts/static/192.0.2.20=dc1.addom.example
```

Auf dem Windows AD DC kann über die DNS-Server Konsole eine sogenannte *Bedingte Weiterleitung* (*Conditional Forwarding*) für die UCS-Domäne eingerichtet werden.

Vertrauensstellungen können nur auf Domänencontrollern eingerichtet werden, gelten dann aber für die gesamte Domäne.

Nach dieser Vorarbeit kann die Vertrauensstellung direkt von der Kommandozeile des UCS Samba/AD DCs eingerichtet werden. In Samba/AD Domänen ist diese Konstellation sehr einfach an der Kommandozeile über das Werkzeug **samba-tool** einzurichten:

```
$ samba-tool domain trust create addom.example \
 -k no -UADDOM\\Administrator%ADAdminPassword \
 --type=external --direction=incoming
```

Mit folgenden Kommandos kann die Vertrauensstellung überprüft werden:

```
$ samba-tool domain trust list
$ wbinfo --ping-dc -domain=addom.example
$ wbinfo --check-secret -domain=addom.example
```

Nach der Einrichtung sollte sich ein Benutzer an Systemen der Windows Active Directory Domäne anmelden können. Als Login-Name muss dabei entweder das Format `UCSDOM\username` oder der Kerberos Prinzipal in der Notation `username@ucsdom.example` angegeben werden.

KAPITEL 10

Identity Management Anbindung an Cloud-Dienste

UCS bietet ein integriertes Identity Management System. Über Univention Management Console können u.a. Benutzer oder Gruppen sehr einfach administriert werden. Abhängig von den installierten Diensten stehen diese Identitäten über unterschiedliche Schnittstellen bereit, z.B. via LDAP.

Mit Hilfe von bereitgestellten Erweiterungen, sogenannten Apps, kann das Managementsystem so erweitert werden, dass Benutzer oder Gruppen auch direkt in Cloud-Dienste repliziert werden. Im App Center sind u.a. Erweiterung für Microsoft 365 oder G Suite vorhanden.

Dank Single Sign-On (SSO) können sich die Benutzer mit ihrem gewohnten Passwort anmelden und anschließend sofort online in der Cloud arbeiten. Dabei bleibt das Passwort im Unternehmensnetzwerk und wird nicht zum Cloud Dienst übertragen.

In den folgenden Kapiteln ist die Einrichtung des Microsoft 365 und des Google Apps for Work Connector beschrieben.

10.1 Microsoft 365 Connector

Der **`Microsoft 365 Connector`** ermöglicht die Synchronisation von Benutzern, Gruppen und Teams mit einer Azure Directory Domain. Über den Connector können Administratoren steuern, welche Benutzerkonten in UCS den Service Microsoft 365 nutzen können. Der Connector stellt die ausgewählten Benutzerkonten in der Azure Active Directory Domäne bereit. Administratoren können konfigurieren, welche Attribute von Benutzerkonten der Connector synchronisiert und welche Attribute der Connector während der Synchronisation anonymisiert.

Der Connector richtet Single Sign-On über den offenen Standard SAML ein. In dieser Konstellation ist UCS der Identity Provider und Microsoft 365 der Service Provider. Nutzer können über Single Sign-On in ihrem Webbrowser auf Microsoft 365 zugreifen, indem sie sich bei UCS anmelden.

Das Authentifizierungsverfahren überträgt keine Passwort-Hashes an Microsoft Azure Cloud. Die Benutzer authentifizieren sich ausschließlich über ihren Webbrowser. Der Webbrowser muss in der Lage sein, die DNS-Einträge der UCS-Domäne aufzulösen, was insbesondere bei mobilen Geräten zu beachten ist.

Wichtig: Das Single Sign-On Setup zwischen UCS und Microsoft 365 nutzt den offenen Standard Security Assertion Markup Language (SAML). Der Webbrowser des Benutzers ist das zentrale Element für die Authentifizierungskommunikation. Daher unterstützen UCS und der **`Microsoft 365 Connector`** Single Sign-On zu Microsoft 365 nur über den Webbrowser des Benutzers.

10.1.1 Einrichtung

Für den Einsatz des Microsoft 365 Connectors wird ein Microsoft 365 Administrator Konto, ein entsprechendes Konto im Azure Active Directory, sowie eine von Microsoft verifizierte Domäne[43] benötigt. Die ersten beiden werden zu Testzwecken kostenlos von Microsoft bereitgestellt. Für das Konfigurieren des SSO wird jedoch eine eigene Internet-Domäne benötigt, in der TXT-Records erstellt werden können.

Falls noch keine Microsoft 365 Subskription vorhanden ist, so kann diese via https://www.office.com/ im Bereich *kostenlos testen für Unternehmen* konfiguriert werden. Mit einem privaten Microsoft Konto ist eine Verbindung nicht möglich.

Anschließend sollte eine Anmeldung mit einem *Microsoft 365 Administratorkonto* im *Microsoft 365 Admin Center* erfolgen. In der linken Navigationsleiste ganz unten ist *Azure AD* auszuwählen, welches in einem neuen Fenster das *Azure Management Portal* öffnet.

Unter dem Menüpunkt *Domänen* kann nun die eigene Domäne hinzugefügt und verifiziert werden. Dafür ist es notwendig, einen TXT-Record im DNS der eigenen Domäne zu erzeugen. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Anschließend sollte der *Status* der konfigurierten Domäne als **überprüft** angezeigt werden.

Nun kann die Microsoft 365 App aus dem App Center auf dem UCS System installiert werden. Die Installation dauert nur wenige Minuten. Anschließend steht ein Einrichtungsassistent (Wizard) für die Einrichtung zur Verfügung. Mit Abschluss des Einrichtungsassistenten ist die Installation abgeschlossen und der Connector ist einsatzbereit.

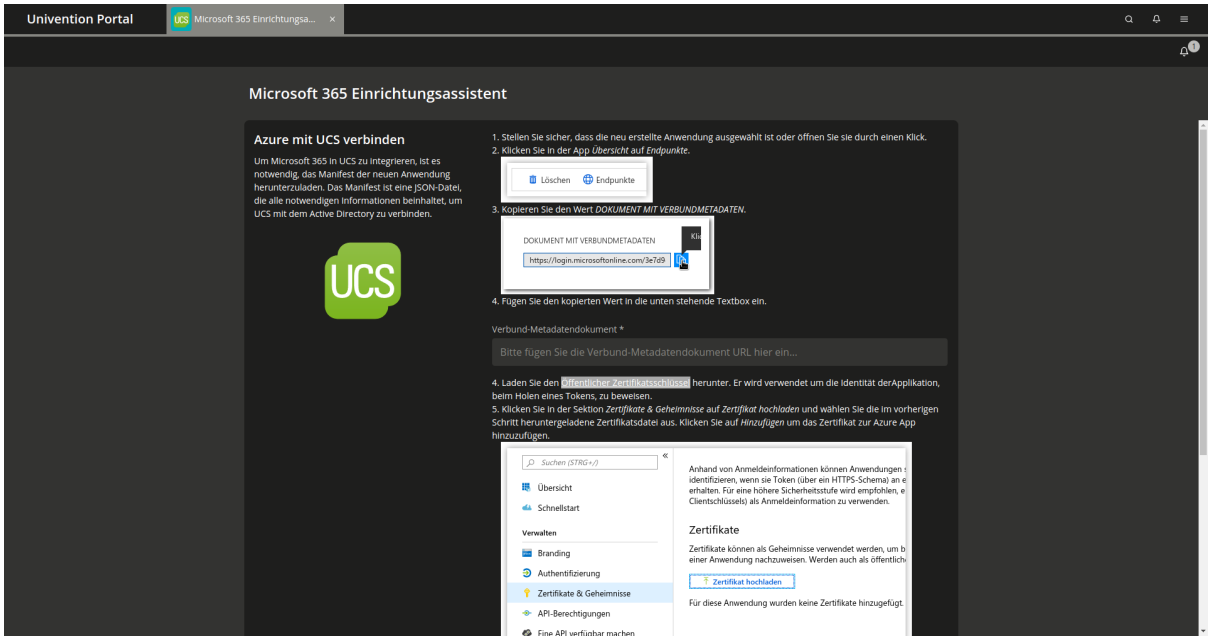


Abb. 10.1: Microsoft 365 Einrichtungsassistent

10.1.2 Konfiguration

Nach der Einrichtung über den Einrichtungsassistenten kann über das Benutzermodul an jedem Benutzerobjekt auf dem Reiter *Microsoft 365* konfiguriert werden, dass dieser Benutzer ins Microsoft 365 provisioniert wird. Der Verbrauch und die Zuweisung von Lizenzen ist im *Microsoft 365 Admin Center* zu erkennen.

[43] https://learn.microsoft.com/de-de/entra/fundamentals/add-custom-domain

Benutzer

Wird eine Änderung am Benutzer durchgeführt, so werden die Änderungen auch in die Azure Active Directory Domäne repliziert. Es erfolgt keine Synchronisation aus dem Azure Active Directory in das UCS System. Das bedeutet, Änderungen, die im Azure Active Directory oder Office Portal vorgenommen werden, können durch Änderungen an den gleichen Attributen in UCS unter Umständen wieder überschrieben werden.

Aufgrund von Sicherheitsrichtlinien des Azure Active Directory können Benutzer oder Gruppen im Azure AD während der Synchronisation nicht gelöscht werden. Sie werden lediglich deaktiviert und umbenannt. Die Lizenzen werden im Azure Active Directory entzogen, so dass diese für andere Benutzer zur Verfügung stehen. Benutzer und Gruppen, deren Namen mit `ZZZ_deleted` anfangen, können im *Microsoft 365 Admin Center* gelöscht werden.

Es ist notwendig in Microsoft 365 ein Land für den Benutzer zu konfigurieren. Der Connector nutzt dafür die Angabe des Landes aus den Kontaktdaten des Benutzers oder, wenn nicht gesetzt, die Einstellung des Servers. Mit Hilfe der Univention Configuration Registry Variable *office365/attributes/usageLocation* (Seite 314) kann ein 2-Zeichen-Kürzel, z.B. `DE` vorgegeben werden.

Über die Univention Configuration Registry Variable *office365/attributes/sync* (Seite 314) wird konfiguriert, welche LDAP Attribute (z.B. Vorname, Nachname) eines Benutzerkontos synchronisiert werden. Es handelt sich um eine kommaseparierte Liste von LDAP Attributen. Somit ist eine Anpassung an die eigenen Bedürfnisse einfach möglich.

Mit der Univention Configuration Registry Variable *office365/attributes/anonymize* (Seite 314) können kommasepariert LDAP Attribute angegeben werden, die zwar im Azure Active Directory angelegt, jedoch mit Zufallswerten gefüllt werden. Die Univention Configuration Registry Variablen *office365/attributes/static/.** (Seite 314) erlauben das Füllen von Attributen auf Microsoft Seite mit einem vordefinierten Wert.

Mit der Univention Configuration Registry Variable *office365/attributes/never* (Seite 314) können kommasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese in *office365/attributes/sync* (Seite 314) oder *office365/attributes/anonymize* (Seite 314) auftauchen.

Die Univention Configuration Registry Variablen *office365/attributes/mapping/.** (Seite 314) definieren eine Abbildung der UCS LDAP Attribute zu Azure Attributen. Diese Variablen müssen normalerweise nicht verändert werden. Die Synchronisation der Gruppen der Microsoft 365 Benutzer kann mit der Univention Configuration Registry Variable *office365/groups/sync* (Seite 314) aktiviert werden.

Änderungen an Univention Configuration Registry Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

Gruppen

Der **`Microsoft 365 Connector`** kann Gruppen mit Microsoft Azure Active Directory synchronisieren. Der Connector synchronisiert eine Gruppe, wenn sie mindestens einen Benutzer enthält, der für *Microsoft 365* aktiviert ist. Standardmäßig erstellt der Connector die Gruppe als `Sicherheitsgruppe` in *Microsoft 365*.

Sie können die Synchronisation aktivieren, indem Sie die Univention Configuration Registry Variable *office365/groups/sync* (Seite 314) auf `yes` setzen.

Neu in Version 5.0-7-erratum-1060: Mit UCS 5.0 erratum 1060[44] können Sie den Gruppentyp auf `Microsoft365 Group` in der UMC auf der Registerkarte *Microsoft 365* ändern.

Wenn das UCS-System, auf dem der Connector installiert ist, nicht mindestens diese Versionsstand hat, können Sie den Gruppentyp nicht ändern.

Wenn Sie den Gruppentyp ändern, löscht der Connector die bestehende Gruppe in *Microsoft 365*, und erstellt eine Gruppe mit dem von Ihnen definierten Gruppentyp. *Microsoft 365* erlaubt es nicht, die Gruppentyp-Eigenschaft einer bestehenden Gruppe zu ändern. Der Connector fügt die Gruppenmitglieder zur Gruppe hinzu, und, wenn die Gruppe ein *Microsoft 365 Team* ist, erstellt der Connector auch das Team.

[44] https://errata.software-univention.de/#/?erratum=5.0x1060

Vorsicht: Das Ändern des Gruppentyps kann sich auf die Berechtigungen und Einstellungen der Gruppe in *Microsoft 365* auswirken. Ändern Sie Gruppentypen mit Vorsicht.

Sie können den Standard-Gruppentyp einer Microsoft 365-Gruppe ändern. Die folgenden Gruppentypen sind verfügbar:

- `Security`
- `Microsoft 365 Group`

Um den Gruppentyp zu ändern, müssen Sie den Standardwert des erweiterten Attributs `UniventionMicrosoft365GroupType` auf einen der verfügbaren Gruppentypen ändern:

```
$ udm settings/extended_attribute modify \
    --dn "cn=UniventionMicrosoft365GroupType,cn=custom attributes,cn=univention,
↪$(ucr get ldap/base)" \
    --set default="Microsoft 365 Group"$ udm settings/extended_attribute modify --
↪dn "cn=UniventionMicrosoft365GroupType,cn=custom attributes,cn=univention,$(ucr␣
↪get ldap/base)" --set default="Microsoft 365 Group"
```

Teams

Für die Nutzung von Teams muss die Synchronisation von Gruppen per Univention Configuration Registry Variable *office365/groups/sync* (Seite 314) mit dem Wert `yes` aktiviert werden, anschließend muss der Dienst Univention Directory Listener neu gestartet werden. Sollen UCS-Gruppen als Teams in Microsoft 365 angelegt werden, so müssen die Gruppen auf dem Reiter *Microsoft 365* über die Checkbox *Microsoft 365 Team* als Team konfiguriert werden. Des Weiteren ist es notwendig, auf demselben Reiter einen Besitzer des Teams zu definieren. Weitere Einstellungen am Team können von den Team-Besitzern direkt im Teams Interface vorgenommen werden. Nach der Aktivierung einer Gruppe als Team werden die Gruppenmitglieder dem neuen Team hinzugefügt. Das Einrichten eines neuen Teams in Microsoft 365 kann einige Minuten in Anspruch nehmen.

Es muss sichergestellt sein, dass die Benutzer eines Teams in Azure eine Lizenz erhalten, in der die Nutzung von Teams enthalten ist.

10.1.3 Synchronisation von Benutzern in mehrere Azure Active Directories

Der Microsoft 365 Connector kann Benutzer in mehrere Azure *Active Directories* synchronisieren. Sind mehrere Verbindungen verfügbar, können an jedem Benutzerkonto individuell die Azure AD Instanzen zugewiesen werden, in denen ein Account erstellt werden soll. Ein Benutzer bekommt in jedem der seinem UCS Konto zugewiesenen Azure AD ein separates Konto mit eindeutigem Benutzernamen (*Userprincipalname*, UPN).

Jede zusätzlich eingerichtete Azure AD Verbindung erhält einen vom Administrator festzulegenden Verbindungsalias als eindeutigen Namen. Für die Verwaltung der Aliase kann das Programm **`/usr/share/univention-office365/scripts/manage_adconnections`** verwendet werden. Ein neuer Alias kann über das Kommando `/usr/share/univention-office365/scripts/manage_adconnections create <Aliasname>` erstellt werden. Dies konfiguriert unter anderem die Univention Configuration Registry Variable *office365/adconnection/wizard* (Seite 314) auf den neu erstellten Alias um. Der Wert dieser Univention Configuration Registry Variable bestimmt, welche Azure Verbindung durch den Microsoft 365 Einrichtungswizard konfiguriert wird.

Nach dem Anlegen muss die Verbindung wie gewohnt über den Microsoft 365 Einrichtungswizard eingerichtet werden, damit Benutzer synchronisiert werden können.

Um Single Sign-On mit mehreren Azure AD Verbindungen zu ermöglichen, muss für jede weitere Verbindung ein neuer logischer SAML Identity Provider erstellt werden. Dies ist in *Erweiterte Konfiguration* (Seite 50) beschrieben.

Der Identity Provider sollte dabei denselben Namen wie der Verbindungsalias erhalten. Wurde ein anderer Name gewählt, muss das PowerShell Skript zur Einrichtung der Single Sign-On Verbindung manuell angepasst werden.

Auf allen für das Single Sign-On der Domäne zuständigen Domaincontrollern muss also beispielsweise die Univention Configuration Registry Variable in der Form `saml/idp/entityID/supplement/Aliasname=true` gesetzt werden.

Ein UCS Benutzer kann in einer Browser-Sitzung nur zu einem Azure AD gleichzeitig verbunden sein. Um die Verbindung zu wechseln, ist ein Abmelden an Microsoft 365 notwendig.

Zur weiteren Konfiguration gibt es die Univention Configuration Registry Variable *office365/defaultalias* (Seite 314). Diese legt fest, in welches Azure AD ein Benutzer- oder Gruppenkonto synchronisiert wird, falls am Benutzerkonto keines explizit ausgewählt wurde. Soll das Konto in ein anderes Azure AD synchronisiert werden, muss bei der Aktivierung für Microsoft 365 das entsprechende Azure AD Verbindungsalias als Ziel ausgewählt werden.

10.1.4 Fehlersuche

Meldungen während der Einrichtung werden in der Logdatei `/var/log/univention/management-console-module-office365.log` protokolliert.

Bei Synchronisationsproblemen sollte die Logdatei des Univention Directory Listener geprüft werden: `/var/log/univention/listener.log`.

Einige Aktionen des Connectors verwenden Operationen der Azure Cloud mit langer Laufzeit, insbesondere bei der Verwendung von Teams. Diese Operationen werden in der Logdatei `/var/log/univention/listener_modules/ms-office-async.log` protokolliert. Mit Hilfe der Univention Configuration Registry Variable *office365/debug/werror* (Seite 314) können mehr Debugausgaben aktiviert werden.

10.2 Google Apps for Work Connector

Der Google Apps for Work Connector ermöglicht die Synchronisation der Benutzer und Gruppen zu einer G Suite Domäne. Dabei lässt sich steuern, welche der in UCS angelegten Benutzer G Suite verwenden dürfen. Die so ausgewählten Benutzer werden entsprechend von UCS in die G Suite Domäne provisioniert. Es kann dabei konfiguriert werden, welche Attribute synchronisiert werden und Attribute können dabei anonymisiert werden.

Die Single Sign-On Anmeldung an G Suite erfolgt über die in UCS integrierte SAML-Implementierung, d.h. die Authentifizierung erfolgt dabei gegen den UCS-Server und es werden keine Passwort-Hashes zur G Suite Domäne übertragen. Die Authentifikation des Benutzers erfolgt ausschließlich über den Webbrowser des Clients. Dieser sollte aber die DNS-Namen der UCS-Domäne auflösen können, das ist insbesondere für Mobilgeräte wichtig zu beachten.

10.2.1 Einrichtung

Für den Einsatz des Google Apps for Work Connectors wird ein G Suite Administrator Konto, ein entsprechendes Konto in der G Suite Domäne, sowie eine von Google verifizierte Domäne[45] benötigt. Die ersten beiden werden zu Testzwecken kostenlos von Google bereitgestellt. Für das Konfigurieren des SSO wird jedoch eine eigene Internet-Domäne benötigt, in der TXT-Records erstellt werden können.

Falls noch keine G Suite Subskription vorhanden ist, so kann diese via Google Workspace für Ihre Organisation einrichten[46] konfiguriert werden. Mit einem privaten Gmail Konto ist eine Verbindung nicht möglich.

Anschließend sollte eine Anmeldung mit einem *G Suite Administratorkonto* in der Admin-Konsole[47] erfolgen. Nun sollte die Verifikation der Domäne erfolgen. Dafür ist es notwendig, einen TXT-Record im DNS der eigenen Domäne zu erzeugen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Nun kann der Google Apps for Work Connector aus dem App Center auf dem UCS System installiert werden. Die Installation dauert nur wenige Minuten. Anschließend steht ein Einrichtungsassistent (Wizard) für die Einrichtung zur Verfügung. Mit Abschluss des Einrichtungsassistenten ist die Installation abgeschlossen und der Connector ist einsatzbereit.

[45] https://support.google.com/a/topic/9196?hl=de
[46] https://support.google.com/a/answer/6365252?hl=de
[47] https://admin.google.com/

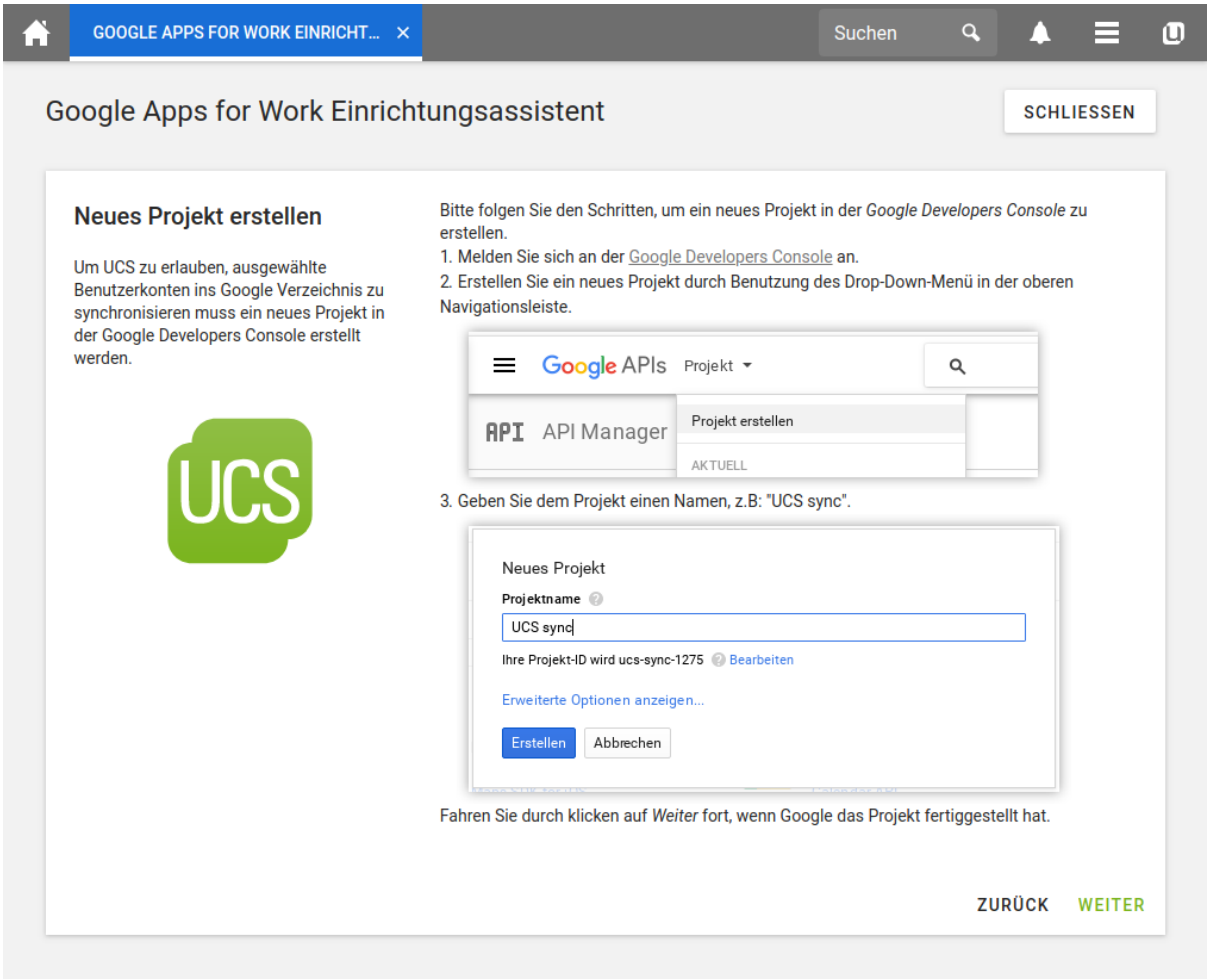


Abb. 10.2: Google Apps for Work Einrichtungsassistent

10.2.2 Konfiguration

Nach der Einrichtung über den Einrichtungsassistenten kann über das Benutzermodul an jedem Benutzerobjekt auf dem Reiter *Google Apps* konfiguriert werden, dass dieser Benutzer zu G Suite provisioniert wird.

Wird eine Änderung am Benutzer durchgeführt, so werden die Änderungen auch in die G Suite Domäne repliziert. Es erfolgt keine Synchronisation aus der G Suite Domäne in das UCS-System. Das bedeutet Änderungen, die in der G Suite Domäne vorgenommen wurden, können durch Änderungen an den gleichen Attributen in UCS unter Umständen wieder überschrieben werden.

Wird bei einem Benutzer die Google Apps Eigenschaft entfernt, so wird der Benutzer entsprechend in der G Suite Domäne gelöscht.

Über die Univention Configuration Registry Variablen *google-apps/attributes/mapping/.** (Seite 306) wird konfiguriert, welche LDAP Attribute (z.B. Vorname, Nachname) eines Benutzerkontos synchronisiert werden. Die Univention Configuration Registry Variable und ihre Werte spiegeln die verschachtelte Datenstruktur der G Suite Benutzerkonten wider. Die Namen, die in den Werten dem Prozentzeichen folgen, sind die Attribute im UCS LDAP. Werden alle Univention Configuration Registry Variablen *google-apps/attributes/mapping/.** (Seite 306) entfernt, so werden keine Daten außer der primären E-Mail-Adresse synchronisiert.

Mit der Univention Configuration Registry Variable *google-apps/attributes/anonymize* (Seite 306) können kommasepariert LDAP Attribute angegeben werden, die zwar in der G Suite Domäne angelegt, jedoch mit Zufallswerten gefüllt werden.

Mit der Univention Configuration Registry Variable *google-apps/attributes/never* (Seite 306) können kommasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese per *google-apps/attributes/mapping/.** (Seite 306) oder *google-apps/attributes/anonymize* (Seite 306) konfiguriert sind.

Die Synchronisation der Gruppen der Google Apps for Work Benutzer kann mit der Univention Configuration Registry Variable *google-apps/groups/sync* (Seite 306) aktiviert werden.

Änderungen an Univention Configuration Registry Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

10.2.3 Fehlersuche

Meldungen während der Einrichtung werden in der folgenden Logdatei `/var/log/univention/management-console-module-googleapps.log` protokolliert.

Bei Synchronisationsproblemen sollte die Logdatei des Univention Directory Listener geprüft werden: `/var/log/univention/listener.log`. Mit Hilfe der Univention Configuration Registry Variable *google-apps/debug/werror* (Seite 306) können mehr Debugausgaben aktiviert werden.

KAPITEL 11

IP- und Netzverwaltung

Dieses Kapitel beschreibt wie IP-Adressen für die in einer UCS-Domäne verwalteten Rechnersysteme zentral über UMC-Module verwaltet und per DHCP zugewiesen werden können.

Netzwerk-Objekte (Seite 219) fassen verfügbare IP-Adressbereiche eines Netzes zusammen. Die DNS-Auflösung sowie die Vergabe von IP-Adressen über DHCP sind in UCS integriert und werden genauer in *Verwaltung von DNS-Daten mit BIND* (Seite 221) sowie *IP-Vergabe über DHCP* (Seite 228) erläutert.

Ein- und ausgehende Netzwerkverbindungen können über die in UCS integrierte *Univention Firewall* auf Basis von **iptable** begrenzt werden (*Paketfilter mit Univention Firewall* (Seite 236)).

Die Integration des Proxy-Servers Squid ermöglicht das Zwischenspeichern von Web-Inhalten und die Umsetzung inhaltlicher Richtlinien für den Web-Zugriff (*Web-Proxy für Caching und Policy Management/Virenscan* (Seite 236)).

11.1 Netzwerk-Objekte

Mit *Netzwerk-Objekten* lassen sich Eigenschaften eines Netzes zentral erfassen, z.B. die verfügbaren IP-Adressen und die DNS- und DHCP-Zonen, in denen die Systeme angesiedelt sind.

So kann beispielsweise ein Netzwerk-Objekt *Produktivnetz* definiert werden, das sich über die IP-Adressen von `192.0.2.0` bis `192.0.2.254` erstreckt. Wird nun ein Windows-Rechnerobjekt angelegt, muss nun nur das Netzwerk-Objekt ausgewählt werden. Es wird dann intern geprüft, welche der IP-Adressen des Netzes bereits vergeben sind und die nächste freie ausgewählt. Wird ein Rechnerobjekt entfernt, wird die Adresse automatisch wieder neu vergeben. Dies erspart dem Administrator eine manuelle Verwaltung verfügbarer Adressen.

Für Netzwerk-Objekte können sowohl IPv4-, als auch IPv6-Adressen verwendet werden. Für mehr Informationen über UMC, siehe *Univention Management Console-Module* (Seite 72).

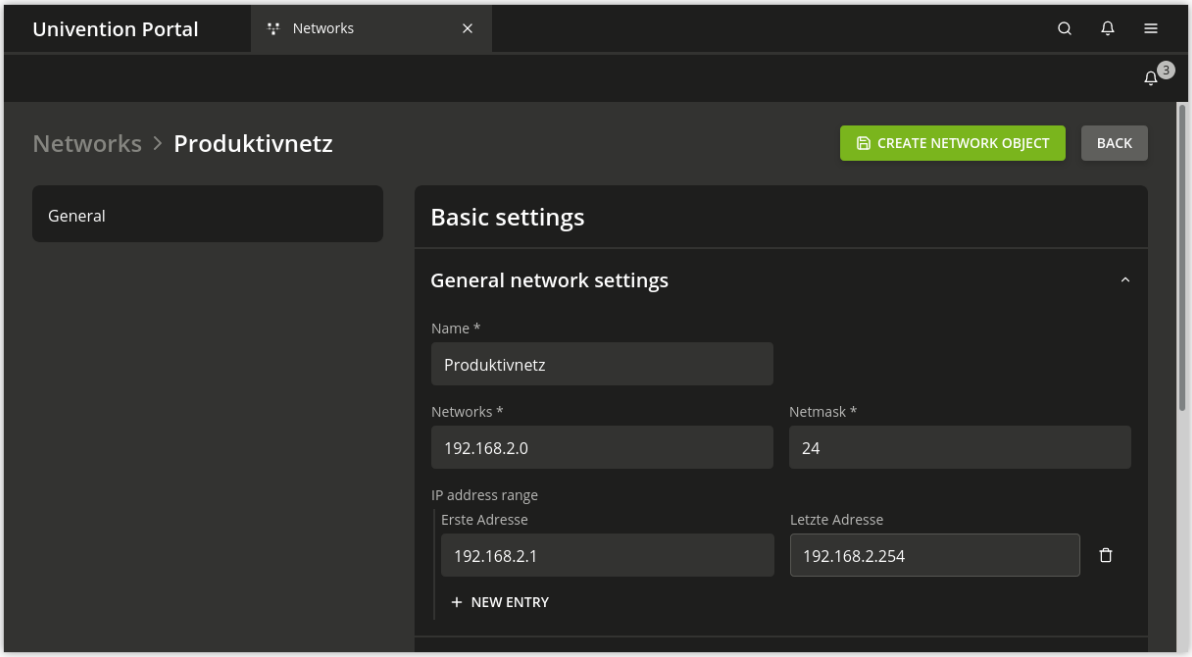


Abb. 11.1: Erstellen eines Netzwerk-Objekts

Tab. 11.1: Reiter *Allgemein*

Attribut	Beschreibung
Name	In diesem Eingabefeld ist der Name des Netzwerks einzutragen. Unter diesem Namen erscheint das Netzwerk auch in der Rechnerverwaltung.
Netzwerk	In diesem Eingabefeld muss die Netzwerk-Adresse in Oktettschreibweise eingetragen werden, z.B. `192.0.2.0`.
Netzmaske	Die Netzmaske kann in diesem Eingabefeld wahlweise als Bitzahl (Netzpräfix) oder in Oktettschreibweise eingetragen werden. Wenn die Netzmaske in Oktettschreibweise eingegeben wird, wird sie automatisch in den entsprechenden Netzpräfix umgewandelt und später auch ausgegeben.
IP-Adressbereich	In diesem Feld können ein oder mehrere IP-Adressbereiche angelegt werden. Wenn später ein Gerät diesem Netzwerk zugeordnet werden soll, wird dem Gerät automatisch die nächste freie IP-Adresse aus den hier eingetragenen IP-Adressbereichen zugewiesen. Wenn an dieser Stelle kein IP-Adressbereich eingerichtet wird, verwendet das System automatisch den Bereich, der sich aus dem Netzwerk und der Netzmaske ergibt. Im Untermenü *DNS-Einstellungen* können Forward Lookup Zone und Reverse Lookup Zone ausgewählt werden. Wird später ein Gerät diesem Netzwerk zugeordnet, wird für das Gerät automatisch ein Host Record in der Forward Lookup Zone beziehungsweise ein Pointer Record in der Reverse Lookup Zone angelegt. Die Zonen werden ebenfalls im UMC-Modul *DNS* verwaltet, siehe *Forward Lookup Zone* (Seite 223). Wird hier keine Zone ausgewählt, werden bei der Zuweisung zu einem Rechnerobjekt keine DNS-Records angelegt. Die DNS-Einträge können aber weiterhin manuell gesetzt werden.
Forward Lookup Zone für DNS-Einträge	Hier ist die Forward Lookup Zone anzugeben, in die Geräte aus diesem Netzwerk eingetragen werden sollen. Über diese Zone wird die Auflösung des Rechnernamens zu einer IP-Adresse durchgeführt.
Reverse Lookup Zone für DNS-Einträge	Hier ist die Reverse Lookup Zone anzugeben, in die Geräte aus diesem Netzwerk eingetragen werden sollen. Über diese Zone wird die Rückwärtsauflösung der IP-Adresse zu einem Rechnernamen durchgeführt.
	Im Untermenü *DHCP-Einstellungen* kann dem Netzwerk ein DHCP-Service zugeteilt werden. Wird später ein Gerät diesem Netzwerk zugeordnet, wird für das Gerät automatisch ein DHCP-Rechner-Eintrag mit der festen IP-Adresse unterhalb des gewählten DHCP-Services angelegt. Die DHCP-Service-Einstellungen werden ebenfalls im UMC-Modul *DHCP*

11.2 Verwaltung von DNS-Daten mit BIND

UCS integriert BIND für die Namensauflösung über das Domain Name System (DNS). Die meisten DNS-Funktionen werden für die DNS-Auflösung in der lokalen Domäne verwendet, die UCS-BIND-Integration kann aber prinzipiell auch für einen öffentlichen Nameserver eingesetzt werden.

Auf allen UCS Directory Node Systemrollen ist BIND immer verfügbar, eine Installation auf anderen Systemrollen wird nicht unterstützt.

Die Konfiguration der von einem UCS-System zu verwendenden Nameserver ist in *Netzwerk Konfiguration* (Seite 155) dokumentiert.

Folgende DNS-Daten werden unterschieden:

Forward Lookup Zone
: Eine *Forward Lookup Zone* enthält Informationen, die zum Auflösen von DNS-Namen in IP-Adressen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen authoritativen, primären Nameserver, dessen Informationen für eine Zone maßgeblich sind. Untergeordnete Server synchronisieren sich mit dem authoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA-Record*.

MX-Record
: Der *MX-Record* einer Forward Lookup Zone ist eine für das E-Mail-Routing notwendige DNS-Information. Er verweist auf den Rechner, der für eine Domäne E-Mails entgegennimmt.

TXT-Records
: *TXT-Records* enthalten menschenlesbaren Text und können beschreibende Informationen zu einer Forward Lookup Zone enthalten.

CNAME-Record
: Ein *CNAME-Record* (desweiteren auch als *Alias-Record* bezeichnet) verweist auf einen vorhandenen, kanonischen DNS-Namen. So kann beispielsweise der kanonische Rechnername des Mailservers einen Alias-Eintrag *mailserver* erhalten, der dann in die Mail-Clients eingetragen wird. Zu einem kanonischen Namen können beliebig viele CNAME-Records definiert werden.

A-Record
: Ein *A-Record* (unter IPv6 *AAAA-Record*) weist einem DNS-Namen eine IP-Adresse zu. A-Records werden in UCS auch als *Host-Records* bezeichnet.

SRV-Record
: Mit einem *SRV-Record* (in UCS als *Service Record* bezeichnet) kann im DNS Informationen über verfügbare Systemdienste hinterlegt werden. In UCS werden Service Records u.a. verwendet, um LDAP-Server oder den Primary Directory Node domänenweit bekannt zu machen.

Reverse Lookup Zone
: Eine *Reverse Lookup Zone* enthält Informationen, die zur Auflösung von IP-Adressen in DNS-Namen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen authoritativen, primären Nameserver, dessen Informationen für eine Zone massgeblich sind. Untergeordnete Server synchronisieren sich mit dem authoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA Record*.

PTR-Record
: Ein *PTR-Record (Pointer Record)* erlaubt die Auflösung einer IP-Adresse in einen Rechnernamen. Er stellt damit in einer Reverse Lookup Zone in etwa das Äquivalent zu einem Host Record in einer Forward Lookup Zone dar.

11.2.1 Konfiguration des BIND-Dienstes

Konfiguration der Debug-Ausgaben von BIND

Der Detailgrad der Debugausgaben von BIND kann über die Univention Configuration Registry-Variablen *dns/debug/level* (Seite 305) und *dns/dlz/debug/level* (Seite 305) (für das Samba-Backend, siehe *Konfiguration des Daten-Backends des Nameservers* (Seite 222)) konfiguriert werden. Die möglichen Werte reichen von `0` (keine Debug-Ausgaben) bis `11`. Eine komplette Aufstellung der Detailgrade findet sich unter Liu and Albitz [13].

Konfiguration des Daten-Backends des Nameservers

In einer typischen BIND-Installation auf einem Nicht-UCS-System wird die Konfiguration durch das Bearbeiten von Zonen-Dateien durchgeführt. In UCS wird BIND komplett über UMC-Module konfiguriert, das seine Daten im LDAP-Verzeichnis speichert.

BIND kann zwei verschiedene Backends für seine Konfigurationsdateien verwenden:

LDAP-Backend
: Das *LDAP-Backend* greift auf die Daten im OpenLDAP-Verzeichnis zu. Dieses Backend ist der Standard. Der DNS-Dienst ist in diesem Fall zweigeteilt: Der *BIND-Proxy* ist der primäre Nameserver und bedient den DNS-Standard-Port `53`. Ein zweiter Server im Hintergrund arbeitet auf Port `7777`. Werden Daten der internen DNS-Zonen im LDAP bearbeitet, wird die Zonendatei auf dem zweiten Server basierend auf den LDAP-Informationen aktualisiert und durch einen Zonentransfer an den BIND-Proxy übertragen.

Samba-Backend
: Samba/AD stellt eine Active Directory-Domäne bereit. Active Directory ist eng mit DNS verknüpft, u.a. für DNS-Updates von Windows-Clients oder für die Lokalisierung der Netlogon-Freigabe. Wird Samba/AD eingesetzt, wird der betreffende UCS Directory Node auf die Verwendung des *Samba-Backend*s umgestellt. Die DNS-Datenbank wird dabei in der Samba-internen LDB Datenbank vorgehalten, die direkt von Samba aktualisiert wird. BIND greift dann über die DLZ Schnittstelle auf die Samba-DNS-Daten zu.

Bei Verwendung des Samba-Backends wird für jede DNS-Anfrage eine Suche im LDAP durchgeführt. Bei Verwendung des OpenLDAP-Backends wird nur bei Änderungen der DNS-Daten im Verzeichnisdienst gesucht. Die Verwendung des LDAP-Backends kann daher zu einer Reduzierung der Systemlast auf Samba/AD-Systemen führen.

Das Backend wird über die Univention Configuration Registry Variable *dns/backend* (Seite 305) konfiguriert. Die DNS-Verwaltung ändert sich durch das verwendete Backend nicht und erfolgt in beiden Fällen über UMC-Module.

Konfiguration von Zonentransfers

In der Grundeinstellung erlaubt der UCS-Nameserver Zonentransfers der DNS-Daten. Ist der UCS-Server aus dem Internet erreichbar, kann dadurch eine Liste aller Rechnernamen und IP-Adressen abgefragt werden. Der Zonentransfer kann bei Verwendung des OpenLDAP-Backends durch Setzen der Univention Configuration Registry Variable *dns/allow/transfer* (Seite 305) auf `none` deaktiviert werden.

11.2.2 Konfiguration der DNS-Daten über Univention Management Console Modul

DNS-Daten werden standardmäßig im Container `cn=dns,`*Basis-DN* abgelegt. Forward- und Reverse-Lookup-Zonen werden direkt in dem Container abgelegt. In den jeweiligen Zonen können zusätzliche DNS-Objekte wie z.B. Pointer-Records angelegt werden.

In Eingabefeldern für Rechner sollte immer der relative oder vollqualifizierte Domänenname und nicht die IP-Adresse des Rechners verwendet werden. Um zu verhindern, dass der Domänenname erneut angehängt wird, sollte ein FQDN immer mit einem Punkt abgeschlossen werden.

In der linken Spalte des UMC-Moduls *DNS* befindet sich eine Liste aller Forward- und Reverse-Lookup-Zonen. Um ein Objekt einer Zone hinzuzufügen - etwa einen Alias-Record zu einer Forward-Zone - muss die entsprechende Zone

ausgewählt werden. Durch *Hinzufügen* wird das Objekt dann in dieser Zone angelegt. Um eine neue Forward- oder Reverse-Zone anzulegen, muss zuerst *Alle DNS-Zonen* selektiert werden, der Klick auf *Hinzufügen* legt dann eine neue Zone an. Wird ein Objekt unterhalb einer Zone angelegt, wird die Zone in den UMC-Dialogen als *übergeordnetes Objekt* bezeichnet.

Forward Lookup Zone

Forward Lookup Zonen enthalten Informationen, die zum Auflösen von DNS-Namen in IP-Adressen verwendet werden. Sie werden im UMC-Modul *DNS* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um eine weitere Forward Lookup Zone anzulegen, muss *Alle DNS-Zonen* selektiert werden und *Hinzufügen* ▸ *DNS: Forward Lookup Zone* ausgewählt werden.

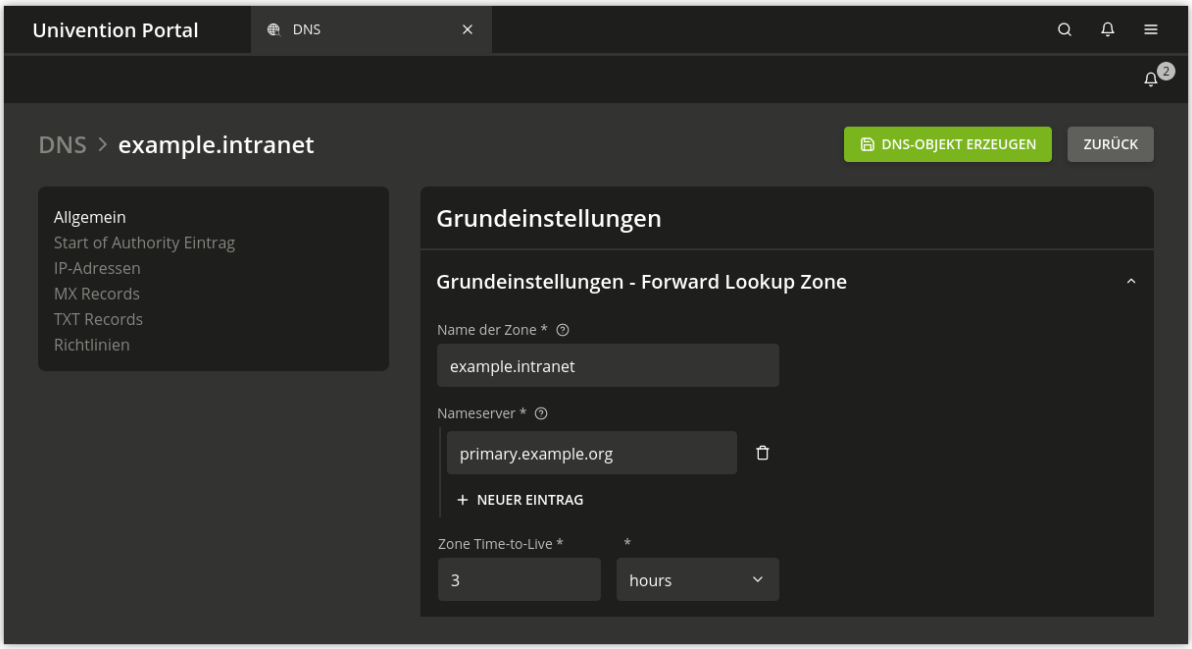


Abb. 11.2: Konfiguration einer Forward Lookup Zone durch Univention Management Console Modul

DNS UMC Modul Forward Lookup - Reiter Allgemein

Tab. 11.2: Reiter *Allgemein*

Attribut	Beschreibung
Name der Zone	Der komplette Name der DNS-Domäne, für die die Zone zuständig sein soll. In Zonennamen **darf** der Domänenname **nicht** mit einem Punkt abgeschlossen werden!
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen. Der Wert wird in Sekunden gespeichert.
Nameserver	Der FQDN mit abschließendem Punkt oder der relative Domänenname der zuständigen Nameserver. Der erste Eintrag in der Liste ist der primäre Nameserver der Zone.

DNS UMC Modul Forward Lookup - Reiter Start of Authority

Tab. 11.3: Reiter *Start of Authority*

Attribut	Beschreibung
Verantwortliche Person	Die E-Mail-Adresse der für die Verwaltung der Zone verantwortlichen Person.
Seriennummer	Anhand der Seriennummer erkennen andere DNS-Server, ob sich Zonendaten geändert haben. Der sekundäre Nameserver vergleicht die Seriennummer seiner Kopie mit der auf dem primären Nameserver. Ist die Seriennummer auf dem sekundären Nameserver niedriger als auf dem primären Nameserver, so kopiert der sekundäre Nameserver die geänderten Daten. Es gibt zwei häufig verwendete Muster für die Seriennummer: • Beginn mit `1` unter Inkrementierung der Seriennummer bei jeder Änderung. • Unter Einbeziehung des Datums kann die Zahl im Format `JJJJMMTTNN` eingegeben werden, wobei – `J` steht für Jahr, – `M` steht für Monat, – `T` steht für Tag – `N` steht für die Nummer der Änderung an diesem Tag steht. Wird die Seriennummer nicht von Hand geändert, wird sie automatisch bei jeder Änderung inkrementiert.
Aktualisierungsintervall	Die Zeitspanne in Sekunden, nach der der sekundäre Nameserver überprüft, ob seine Kopie der Zonendaten noch aktuell ist.
Intervall für erneute Versuche	Die Zeitspanne in Sekunden, nach der der sekundäre Nameserver nach einer fehlgeschlagenen Aktualisierungsanfrage erneut versucht, die Aktualität seiner Zonendaten-Kopie zu überprüfen. Üblicherweise wird diese Zeitspanne kürzer gewählt als das Aktualisierungsintervall, darf aber auch gleich lang sein.
Ablaufintervall	Die Zeitspanne in Sekunden, nach der die Zonendaten-Kopie auf dem sekundären Nameserver ungültig wird, wenn ihre Aktualität nicht überprüft werden konnte. Bei einem Ablaufintervall von einer Woche bedeutet dies beispielsweise, dass die Zonendaten-Kopie ungültig wird, wenn eine Woche lang alle Aktualisierungsanfragen fehlgeschlagen sind. In dem Fall wird davon ausgegangen, dass die Daten nach der Ablaufzeit zu veraltet sind, um weiter verwendet zu werden. Der sekundäre Nameserver kann dann keine Namensauflösungsanfragen für diese Zone mehr beantworten.
Negative Time-to-Live	Die negative *Time-to-Live* gibt in Sekunden an, wie lange andere Server *No-such-Domain*-Antworten (NXDOMAIN) im Cache behalten dürfen. Der Wert darf nicht mehr als 3 Stunden betragen, der Standard sind 3 Stunden.

DNS UMC Modul Forward Lookup - Reiter IP Adressen

Tab. 11.4: Reiter *IP Adressen*

Attribut	Beschreibung
IP Adressen	Mit diesem Eingabefeld können eine oder mehrere IP-Adressen angegeben werden, die zurückgegeben werden, wenn der Name der Zone aufgelöst wird. Die hier hinterlegten Adressen werden von Microsoft Windows-Clients in AD-kompatiblen Domänen abgefragt.

DNS UMC Modul Forward Lookup - Reiter MX Records

Tab. 11.5: Reiter *MX Records*

Attribut	Beschreibung
Priorität	Ein Zahlenwert zwischen 0 und 65535. Stehen mehrere Mail-Server für den MX-Record zur Verfügung, wird zuerst versucht, den Server mit dem niedrigsten Prioritätswert in Anspruch zu nehmen.
Mail-Server	Hier wird der für diese Domäne zuständige Mail-Server als vollqualifizierter Domänenname mit abschließendem Punkt eingetragen. Es dürfen nur kanonische Namen und keine Alias-Namen verwendet werden.

DNS UMC Modul Forward Lookup - Reiter TXT Records

Tab. 11.6: Reiter *TXT Recods*

Attribut	Beschreibung
TXT Record	Ein beschreibender Text zu dieser Zone. Text Records dürfen keine Umlaute oder sonstige Sonderzeichen enthalten.

CNAME-Record (Alias-Records)

CNAME-Records / Alias-Records werden im UMC-Modul *DNS* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit *Hinzufügen* ▸ *DNS: Alias Record* kann dann ein neuer Record angelegt werden.

Tab. 11.7: Reiter *Allgemein*

Attribut	Beschreibung
Alias	Der Aliasname als FQDN mit abschließendem Punkt oder als relativer Domänenname, der auf den kanonischen Namen verweisen soll.
Kanonischer Name	Der kanonische Name des Rechners, auf den der Alias verweisen soll, angegeben als FQDN mit abschließendem Punkt oder als relativer Domänenname.

A/AAAA-Records (Host Records)

Host-Records werden im UMC-Modul *DNS* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit *Hinzufügen* ▸ *DNS: Host Record* kann dann ein neuer Record angelegt werden.

Beim Hinzufügen oder Bearbeiten eines Rechner-Objekts kann ein Host Record automatisch erstellt oder geändert werden.

Tab. 11.8: Reiter *Allgemein*

Attribut	Beschreibung
Rechnername	Der FQDN mit abschließendem Punkt oder der relative Domänenname des Rechners.
IP Adressen	Die IPv4 und/oder IPv6-Adressen, auf die der Host Record verweisen soll.
Zone Time-to-Live	Die Time-to-Live gibt in Sekunden an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

Service Records

Service Records werden im Modul *DNS* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit *Hinzufügen* ▸ *DNS: Service Record* kann dann ein neuer Record angelegt werden.

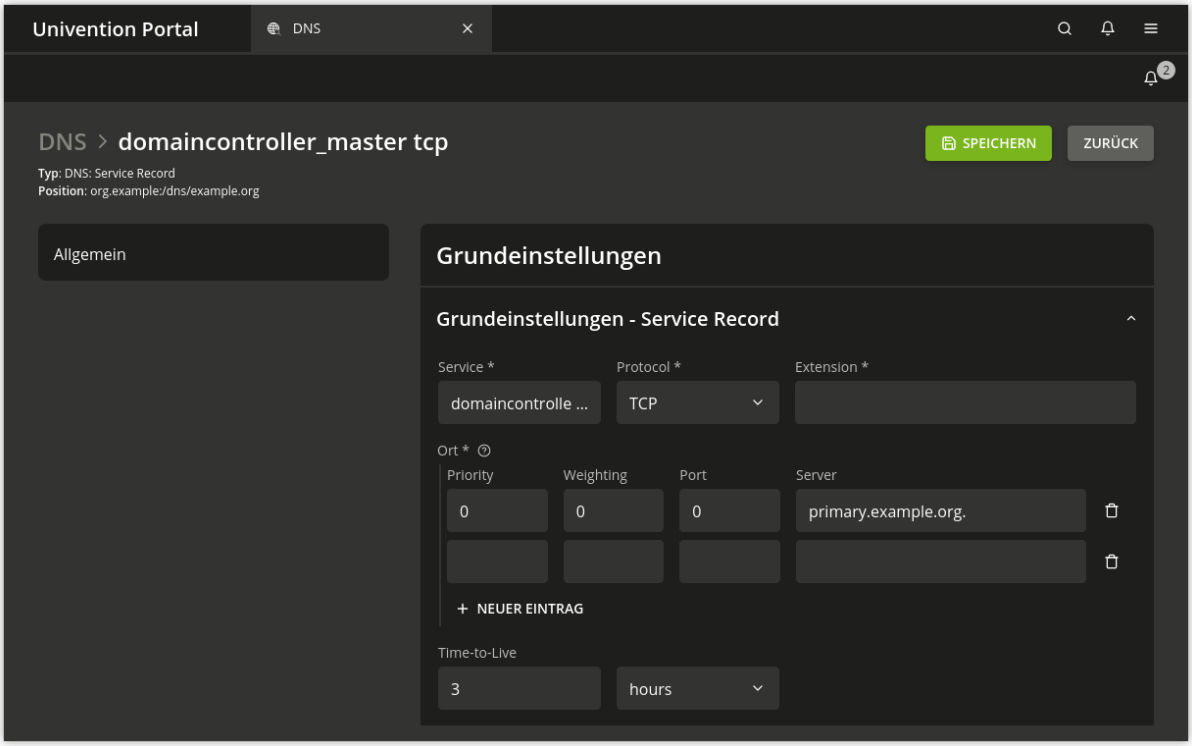


Abb. 11.3: Konfiguration eines Service Records

Ein Service Record muss immer einer Forward Lookup Zone zugewiesen sein und kann daher nur einer Forward Lookup Zone oder einem untergeordneten Container zugewiesen werden.

Tab. 11.9: Reiter *Allgemein*

Attribut	Beschreibung
Dienst	Der Name, unter dem der Dienst erreichbar sein soll.
Protokoll	Das Protokoll, über das der Record erreichbar ist (`TCP`, `UDP`, `MSDCS` oder `SITES`).
Erweiterung	Über dieses Eingabefeld können weitere Parameter übergeben werden.
Priorität	Eine ganze Zahl zwischen 0 und 65535. Stellen mehrere Server denselben Dienst zur Verfügung, wendet sich der Client zuerst an den Server mit dem niedrigeren Prioritätswert.
Gewichtung	Eine ganze Zahl zwischen 0 und 65535. Die Gewichtung dient der Lastverteilung zwischen Servern mit gleicher Priorität. Wenn mehrere Server denselben Dienst zur Verfügung stellen und denselben Prioritätswert haben, wird die Last im Verhältnis der Gewichtungen auf die Server verteilt. Beispiel: `Server1` hat eine Priorität von 1 und eine Gewichtung von 1, während `Server2` ebenfalls eine Priorität von 1, aber eine Gewichtung von 3 hat. In diesem Fall wird `Server2` dreimal so oft verwendet wie `Server1`. Die Belastung wird abhängig vom Dienst beispielsweise als Anzahl der Anfragen oder Verbindungen gemessen.
Port	Der Port, über den der Dienst auf dem Server zu erreichen ist (gültige Werte liegen zwischen 1 und 65535).
Server	Der Name des Servers, auf dem der Dienst bereitgestellt wird, als FQDN mit abschließendem Punkt oder als relativer Domänenname. Für jeden Dienst können über die Auswahlbox auch mehrere Server eingetragen werden.
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

Reverse Lookup Zone

Eine Reverse Lookup Zone dient zur Umwandlung von IP-Adressen in Rechnernamen. Sie werden im UMC-Modul *DNS* verwaltet. Um eine weitere Reverse Lookup Zone anzulegen, muss *Alle DNS-Zonen* selektiert werden und *Hinzufügen ▸ DNS: Reverse Lookup Zone* ausgewählt werden.

DNS UMC Modul Reverse Lookup - Reiter Allgemein

Tab. 11.10: Reiter *Allgemein*

Attribut	Beschreibung
Subnetz	Die IP-Adresse des Netzwerkes, für das die Reverse Lookup Zone gültig sein soll. Wenn beispielsweise das betreffende Netz aus den IP-Adressen `192.0.2.0` bis `192.0.2.255` besteht, wäre `192.0.2` einzutragen.
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

Jede DNS-Zone hat mindestens einen autoritativen, primären Nameserver, dessen Informationen die Zone regeln. Untergeordnete Server synchronisieren sich mit dem autoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone definiert, wird in der DNS-Terminologie als SOA Eintrag bezeichnet.

DNS UMC Modul Reverse Lookup - Reiter Start of Authority

Tab. 11.11: Reiter *Start of Authority*

Attribut	Beschreibung
Verantwortliche Person	Die E-Mail-Adresse der für die Verwaltung der Zone verantwortlichen Person (mit abschließendem Punkt).
Nameserver	Der FQDN mit abschließendem Punkt oder der relative Domänenname der zuständigen Nameserver. Der erste Eintrag in der Liste ist der primäre Nameserver der Zone.
Seriennummer	Siehe die Dokumentation zu Forward Lookup Zonen in *Forward Lookup Zone* (Seite 223).
Aktualisierungsintervall	Siehe die Dokumentation zu Forward Lookup Zonen in *Forward Lookup Zone* (Seite 223).
Intervall für erneute Versuche	Siehe die Dokumentation zu Forward Lookup Zonen in *Forward Lookup Zone* (Seite 223).
Ablaufintervall	Siehe die Dokumentation zu Forward Lookup Zonen in *Forward Lookup Zone* (Seite 223).
Minimum Time-to-Live	Siehe die Dokumentation zu Forward Lookup Zonen in *Forward Lookup Zone* (Seite 223).

Pointer Records

Pointer-Records werden im UMC-Modul *DNS* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Reverse Lookup Zone ausgewählt werden. Mit *Hinzufügen* ▸ *DNS: Pointer Record* kann dann ein neuer Record angelegt werden.

Tab. 11.12: Reiter *Allgemein*

Attribut	Beschreibung
Adresse	Das letzte Oktett der IP-Adresse des Rechners (abhängig vom Netz-Präfix, siehe unten).
Pointer	Der FQDN des Rechners mit abschließendem Punkt. In einem Netzwerk mit 24-Bit langem Netz-Präfix (Netzmaske `255.255.255.0`) soll für den Rechner `client001` mit der IP-Adresse `192.0.2.101` ein Pointer angelegt werden. In das Feld *Adresse* ist dann `101` und in *Pointer* `client001.firma.com.` einzutragen. Beispiel: Bei einem Netzwerk mit 16-Bit langem Netz-Präfix (Netzmaske `255.255.0.0`) müssten für diesen Rechner die letzten zwei Oktette in umgekehrter Reihenfolge (hier `101.1`) eingetragen werden. In das Feld *Pointer* wäre auch hier `client001.firma.com.` einzutragen.

11.3 IP-Vergabe über DHCP

Das Dynamic Host Configuration Protocol (DHCP) weist Rechnern eine IP-Adresse, die Subnetz-Maske und gegebenenfalls weitere Einstellungen wie Gateway oder NetBIOS-Server zu. Die IP-Adresse kann fest oder dynamisch vergeben werden.

Die Verwendung von DHCP ermöglicht eine zentrale Vergabe und Kontrolle von IP-Adressen über das LDAP-Verzeichnis ohne manuelle Einträge an den einzelnen Rechnersystemen vorzunehmen.

Die DHCP-Integration in UCS unterstützt nur IPv4.

In einem *DHCP-Service* werden DHCP-Server mit einer gemeinsamen LDAP-Konfiguration zusammengefasst. Globale Konfigurationsparameter werden am DHCP-Service angegeben, spezifische Parameter in den Objekten darunter.

Ein DHCP-Server kann mit der Applikation *DHCP-Server* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **univention-dhcp** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Jeder DHCP-Server verteilt IP-Adressen über DHCP. In der Grundeinstellungen werden nur statische IP-Adressen an im UCS-LDAP registrierte Rechnerobjekte vergeben.

Werden ausschließlich feste IP-Adressen vergeben, können beliebig viele DHCP-Server in einem DHCP-Service verwendet werden. Alle DHCP-Server greifen auf identische Daten aus dem LDAP zurück und bieten den DHCP-Clients die Daten mehrfach an. DHCP-Clients akzeptieren dann die erste Antwort und verwerfen die übrigen.

Werden auch dynamisch IP-Adressen verteilt, muss der DHCP-Failover-Mechanismus eingesetzt werden. Dabei können maximal zwei DHCP-Server pro Subnetz verwendet werden.

Mit einem *DHCP-Rechner*-Eintrag wird ein Rechner dem DHCP-Service bekannt gemacht. Für Rechner, die per DHCP eine feste IP-Adresse beziehen sollen, ist ein DHCP-Rechner-Objekt zwingend erforderlich. DHCP-Rechner-Objekte müssen in der Regel nicht manuell erstellt werden, weil diese automatisch angelegt werden, wenn einem Rechnerobjekt mit fester IP-Adresse ein DHCP-Service zugewiesen wird.

Für jedes Subnetz wird ein *DHCP-Subnetz*-Eintrag benötigt, unabhängig davon, ob dynamische IP-Adressen aus diesen Subnetzen vergeben werden sollen.

Über die Einrichtung von *DHCP-Pools* innerhalb von Subnetzen können den verschiedenen IP-Adressbereichen unterschiedliche Konfigurationsparameter zugeordnet werden. Auf diese Weise können unbekannte Rechner in einem IP-Adressbereich zugelassen und von einem anderen IP-Adressbereich ausgeschlossen werden. DHCP-Pools können nur unterhalb von DHCP-Subnetz-Objekten angelegt werden.

Falls mehrere IP-Subnetze gemeinsam dasselbe physikalische Ethernet-Netzwerk verwenden, sollten diese als *DHCP Shared Subnet* unterhalb eines *DHCP Shared Network* eingetragen werden. *DHCP Shared Subnet*-Objekte können nur unterhalb von *DHCP Shared Network*-Objekten angelegt werden.

Werte, die auf einer Ebene der DHCP-Konfiguration angegeben werden, gelten immer für diese und alle darunterliegenden Ebenen, sofern dort keine anderen Angaben gemacht werden. Ähnlich wie bei Richtlinien gilt immer der Wert, der dem Objekt am nächsten ist.

11.3.1 Aufbau der DHCP-Konfiguration durch DHCP-LDAP-Objekte

In der linken Spalte des UMC-Moduls *DHCP* befindet sich eine Liste aller DHCP-Services. Um einem DHCP-Service ein Objekt hinzuzufügen - etwa ein weiteres Subnetz - muss der entsprechende Service ausgewählt werden. Durch *Hinzufügen* wird das Objekt dann in diesem Service angelegt. Um einen neuen DHCP-Service anzulegen, muss zuerst *Alle DHCP-Dienste* selektiert werden, der Klick auf *Hinzufügen* legt dann einen neue Service an. Wird ein Objekt unterhalb eines Services angelegt, wird der Service in den UMC-Dialogen als *übergeordnetes Objekt* bezeichnet.

Verwaltung von DHCP-Services

DHCP-Services werden im UMC-Modul *DHCP* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen neuen DHCP-Service anzulegen muss zuerst *Alle DHCP-Dienste* in der linken Spalte des UMC-Moduls selektiert werden. Ein Klick auf *Hinzufügen* legt dann einen neue Service an.

Ein DHCP-Server kann nur einen DHCP-Service bedienen; wenn ein weiterer DHCP-Service verwendet werden soll, muss dafür ein separater DHCP-Server eingerichtet werden (siehe *Verwaltung von DHCP-Server-Einträgen* (Seite 230)).

Am DHCP-Service-Objekt werden häufig folgende Parameter festgelegt, die dann für alle Rechner gültig sind, die von diesem DHCP-Service bedient werden (es sei denn, es werden auf tieferen Ebenen andere Angaben gemacht):

- *Domänenname* und *DNS-Server* unter *Richtlinie: DHCP DNS*
- *NetBIOS-Nameserver* unter *Richtlinie: DHCP NetBIOS*

Eine Beschreibung dieser und der anderen DHCP-Richtlinien findet sich unter *Konfiguration von Clients durch DHCP-Richtlinien* (Seite 233).

Tab. 11.13: Reiter *Allgemein*

Attribut	Beschreibung
Service-Name	In dieses Eingabefeld muss ein beliebiger, aber eindeutiger Name für den DHCP-Service eingetragen werden, z.B. `firma.com`.

Verwaltung von DHCP-Server-Einträgen

Jeder Server, der den DHCP-Dienst anbieten soll, benötigt zwingend einen *DHCP-Server*-Eintrag im LDAP-Verzeichnis. Der Eintrag muss in der Regel nicht von Hand angelegt werden, sondern wird durch das Join-Skript des **`univention-dhcp`**-Pakets angelegt. Um dennoch manuell einen weiteren Record anzulegen, muss im UMC-Modul *DHCP* in der linken Spalte ein DHCP-Service ausgewählt werden. Mit *Hinzufügen* ▸ *DHCP Server* kann dann ein neuer Server registriert werden.

Tab. 11.14: Reiter *Allgemein*

Attribut	Beschreibung
Server-Name	In diesem Eingabefeld ist der Rechnername, der den DHCP-Dienst anbieten soll, einzutragen, z.B. `ucs-primary`. Ein Server kann immer nur einen einzigen DHCP-Dienst anbieten und kann deshalb nicht gleichzeitig in mehreren DHCP-Services eingetragen sein.

Verwaltung von DHCP-Subnetzen

DHCP-Subnetze werden im UMC-Modul *DHCP* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um ein weiteres Subnetz anzulegen, muss in der linken Spalte ein DHCP-Service ausgewählt werden. Mit *Hinzufügen* ▸ *DHCP: Subnetz* kann dann ein neues Subnetz angelegt werden.

Ein DHCP-Subnetz-Eintrag ist für jedes Subnetz, aus dem dynamische oder feste IP-Adressen vergeben werden sollen, zwingend erforderlich. Das Eintragen von IP-Adressbereichen ist nur notwendig, wenn IP-Adressen dynamisch vergeben werden sollen.

Falls *DHCP:Shared Subnet*-Objekte verwendet werden sollen, sollten die entsprechenden Subnetze unterhalb des dafür angelegten *DHCP:Shared Network*-Containers angelegt werden (siehe *Verwaltung von DHCP Shared Networks / DHCP Shared Subnets* (Seite 233)).

Tab. 11.15: Reiter *Allgemein*

Attribut	Beschreibung
Subnetz-Adresse	In diesem Eingabefeld ist die IP-Adresse des Subnetzes in Oktettschreibweise einzutragen, z.B. `192.0.2.0`.
Netzmaske	Die Netzmaske kann in diesem Eingabefeld wahlweise als Dezimalzahl des Netzpräfix oder in Oktettschreibweise eingetragen werden. Wenn die Netzmaske in Oktettschreibweise eingegeben wird, wird sie automatisch in den entsprechenden Netzpräfix umgewandelt und später auch ausgegeben.
Dynamische Adresszuweisung	Hier können ein einzelner oder mehrere IP-Adressbereiche eingerichtet werden, die für die dynamische Vergabe zur Verfügung stehen. Der Bereich erstreckt sich von *Erste Adresse* bis *Letzte Adresse* in Oktettschreibweise. **Vorsicht:** Dynamische IP-Adressbereiche für ein Subnetz sind immer entweder ausschließlich im Subnetz-Eintrag oder ausschließlich in einem oder mehreren gesonderten Pool-Einträgen anzugeben. Die Typen der Einträge im IP-Adressbereich innerhalb eines Subnetzes dürfen nicht gemischt werden! Wenn in einem Subnetz verschiedene IP-Adressbereiche mit unterschiedlichen Konfigurationen eingesetzt werden sollen, müssen dafür Pool-Einträge angelegt werden.

Auf dieser Ebene wird häufig über dir Karteikarte *Richtlinie: DHCP Routing* das Gateway für alle Rechner in diesem Subnetz festgelegt (es sei denn, es werden an DHCP-Pools andere Angaben gemacht).

Verwaltung von DHCP-Pools

DHCP-Pools können nur über das UMC-Modul *LDAP-Verzeichnis* verwaltet werden. Dazu muss in ein DHCP-Subnetz-Objekt navigiert werden - ein DHCP-Pool-Objekt muss immer unterhalb eines DHCP-Subnetz-Objektes angelegt werden - und dort mit *Hinzufügen* ein *DHCP: Pool*-Objekt eingefügt werden.

Wenn in einem Subnetz DHCP-Pools angelegt werden, sollten keine IP-Adressbereiche im Subnetz-Eintrag definiert werden. Diese sind ausschließlich in den Pool-Einträgen anzulegen.

Reiter Allgemein

Tab. 11.16: Reiter *Allgemein*

Attribut	Beschreibung
Name	In dieses Eingabefeld muss ein beliebiger, aber eindeutiger Name für den DHCP-Pool eingetragen werden, z.B. `testnetz.firma.com`.
Dynamischer Bereich	Hier können die IP-Adressen in Oktettschreibweise angegeben werden, die dynamisch vergeben werden.

Reiter Erweiterte Einstellungen

Tab. 11.17: Reiter *Erweiterte Einstellungen*

Attribut	Beschreibung
Failover Peer	Der Name einer Failover-Konfiguration, die von Hand in der Datei `/etc/dhcp/local.conf` konfiguriert werden. Hinweise zur Einrichtung finden sich in A Basic Guide to Configuring DHCP Failover[48].
Erlaube bekannte Clients	Ein Computer wird durch seine MAC-Adresse identifiziert. Ist dieses Feld auf `erlauben` gesetzt oder nicht gesetzt, ist ein Computer mit einem DHCP-Rechner-Eintrag (siehe *Registrierung von Rechnern mit DHCP-Rechner-Objekten* (Seite 232)) berechtigt eine IP-Adresse aus diesem Pool zu beziehen. Ist es auf `verbieten` gesetzt, erhalten diese Computer keine IP-Adresse aus dem Pool.
Erlaube unbekannte Clients	Ein Computer wird durch seine MAC-Adresse identifiziert. Ist dieses Feld auf `erlauben` gesetzt oder nicht gesetzt, ist ein Computer ohne DHCP-Rechner-Eintrag (siehe *Registrierung von Rechnern mit DHCP-Rechner-Objekten* (Seite 232)) berechtigt eine IP-Adresse aus diesem Pool zu beziehen. Ist es auf `verbieten` gesetzt, erhalten diese Computer keine IP-Adresse aus dem Pool.
Dynamische BOOTP-Clients erlauben	BOOTP ist das Vorgängerprotokoll von DHCP. Es kennt keinen Mechanismus zum Aktualisieren eines Leases und weist Adressen zeitlich unbeschränkt zu, was den Pool erschöpfen kann. Ist diese Option auf `erlauben` gesetzt können Clients auch über BOOTP eine Adresse aus diesem Pool zu beziehen.
Alle Clients	Wird diese Option auf `verbieten` gesetzt, wird der Pool global deaktiviert. Diese Option ist nur in Ausnahmefällen sinnvoll.

Registrierung von Rechnern mit DHCP-Rechner-Objekten

Mit einem *DHCP Rechner*-Eintrag wird der betreffende Rechner im DHCP-Service registriert. Rechner können in Abhängigkeit von ihrem Registrierungsstatus behandelt werden. Bekannte Rechner können feste oder dynamische IP-Adressen vom DHCP-Service beziehen; unbekannte Rechner erhalten nur dynamische IP-Adressen.

Üblicherweise werden beim Hinzufügen eines Rechners über die Rechnerverwaltung automatisch DHCP-Rechner-Einträge erstellt. Unterhalb des DHCP-Service-Objekts gibt es die Möglichkeit, manuell DHCP-Rechner-Einträge hinzuzufügen oder bestehende Einträge, egal ob manuell oder automatisch erzeugt, zu bearbeiten.

DHCP-Rechner-Objekte werden im UMC-Modul *DHCP* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um einen Rechner manuell im DHCP zu registrieren, muss in der linken Spalte des Moduls ein DHCP-Service ausgewählt werden. Mit *Hinzufügen* ▸ *DHCP: Rechner* kann dann ein Rechner registriert werden.

[48] https://kb.isc.org/docs/aa-00502

Tab. 11.18: Reiter *Allgemein*

Attribut	Beschreibung
Rechnername	In diesem Eingabefeld ist ein Name für den Rechner einzugeben (der in der Regel auch einen Eintrag in der Rechnerverwaltung besitzt). Es empfiehlt sich, in beiden Einträgen denselben Namen und dieselbe MAC-Adresse für den Rechner zu verwenden, um die Zuordnung zu erleichtern.
Netzwerktyp	In dieser Auswahlliste ist der Typ des verwendeten Netzwerks auszuwählen. Hier ist nahezu immer *Ethernet* auszuwählen.
Adresse	In diesem Eingabefeld ist die MAC-Adresse der Netzwerkkarte einzutragen, z.B. `2e:44:56:3f:12:32` oder `e-44-56-3f-12-32`.
Feste IP-Adressen	Hier können dem Rechner eine oder mehrere feste IP-Adressen zugewiesen werden. Neben einer IP-Adresse kann auch ein vollqualifizierter Domänenname angegeben werden, der vom DHCP-Server in eine oder mehrere IP-Adressen aufgelöst wird.

Verwaltung von DHCP Shared Networks / DHCP Shared Subnets

DHCP Shared Network-Objekte nehmen Subnetze auf, die ein physikalisches Netzwerk gemeinsam nutzen.

DHCP-Shared-Network-Objekte werden im UMC-Modul *DHCP* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)). Um ein Shared Network anzulegen, muss in der linken Spalte des Moduls ein DHCP-Service ausgewählt werden. Mit *Hinzufügen* ▸ *DHCP: Shared Network* kann dann ein Netzwerk registriert werden.

Vorsicht: Ein Shared-Network muss mindestens einen Shared-Subnet-Eintrag enthalten. Anderenfalls beendet sich der DHCP-Dienst und kann nicht gestartet werden, bis die Konfiguration korrigiert ist.

Tab. 11.19: Reiter *Allgemein*

Attribut	Beschreibung
Shared Network Name	In dieses Eingabefeld ist ein Name für das Shared Network einzutragen.

Als *DHCP:Shared Subnet* werden Subnetze deklariert, die gemeinsam dasselbe physikalische Netzwerk verwenden. Alle Subnetze, die dasselbe Netzwerk verwenden, müssen unterhalb desselben Shared Network-Containers angelegt werden. Für jedes Subnetz ist ein eigenes *DHCP:Shared Subnet*-Objekt anzulegen.

DHCP-Shared-Subnet-Objekte können nur über das UMC-Modul *LDAP-Verzeichnis* verwaltet werden. Dazu muss in ein DHCP-Shared Network-Objekt navigiert werden - ein DHCP-Shared Subnet-Objekt muss immer unterhalb eines DHCP-Shared Network-Objektes angelegt werden - und dort mit *Hinzufügen* ein *DHCP: Shared Subnet*-Objekt eingefügt werden.

11.3.2 Konfiguration von Clients durch DHCP-Richtlinien

Bemerkung: Viele Einstellungen für DHCP werden über Richtlinien konfiguriert. Diese finden auch Anwendung auf DHCP-Rechner-Objekte, wenn eine Richtlinie mit der LDAP-Basis oder einem der anderen dazwischenliegenden Container verknüpft ist. Da die Einstellungen an DHCP-Rechner-Objekte die höchste Priorität haben, werden andere Einstellungen an Subnetz- oder Service-Objekten ignoriert.

DHCP-Richtlinien sollten von daher direkt mit den DHCP-Netzwerk-Objekten (z.B. den DHCP-Subnetzen) verknüpft werden.

Alternativ kann in den erweiterten Einstellungen der Richtlinien unter *Objekt* ▸ *Ausgeschlossene Objektklassen* die LDAP-Klasse `univentionDhcpHost` hinzugefügt werden. Solche Richtlinien finden dann nicht länger auf die

DHCP-Rechner-Objekte Anwendung, wodurch dann die Einstellungen aus DHCP-Subnetz und -Service benutzt werden.

Tipp: Bei Verwendung der Kommandozeile **udm dhcp/host list** (siehe auch *DNS/DHCP* (Seite 90)) kann die Option `--policies 0` verwendet werden, um die effektiven Einstellungen anzeigen zu lassen.

Vorgabe des Gateways

Das Default-Gateway kann per DHCP über eine Richtlinie vom Typ *DHCP Routing* festgelegt werden, die im UMC-Modul *Richtlinien* verwaltet wird (siehe auch *Richtlinien* (Seite 77)).

Tab. 11.20: Reiter *Allgemein*

Attribut	Beschreibung
Router	Hier sind die Namen oder IP-Adressen der Router einzutragen. Dabei ist darauf zu achten, dass der DHCP-Server diese Namen in IP-Adressen auflösen kann. Die Router werden vom Client in der Reihenfolge angesprochen, in der sie in der Auswahlliste erscheinen.

Vorgabe der DNS-Server

Die von einem Client zu verwendenden Nameserver können per DHCP über eine Richtlinie vom Typ *DHCP DNS* festgelegt werden, die im UMC-Modul *Richtlinien* verwaltet wird (siehe auch *Richtlinien* (Seite 77)).

Tab. 11.21: Reiter *Allgemein*

Attribut	Beschreibung
Domänenname	Der Name der Domäne, den der Client automatisch an Rechnernamen anhängt, die er zur Auflösung an den DNS-Server schickt und die keine vollqualifierten Domänennamen sind. Üblicherweise wird hier der Name der Domäne verwendet, der der Client angehört.
DNS-Server	Hier können IP-Adressen oder vollqualifizierte Domänennamen (FQDNs) von DNS-Servern hinzugefügt werden. Bei der Verwendung von FQDNs ist darauf zu achten, dass der DHCP-Server die Namen in IP-Adressen auflösen kann. Die DNS-Server werden von den Clients entsprechend der hier angegebenen Reihenfolge kontaktiert.

Vorgabe des WINS-Server

Der zu verwendende WINS-Server kann per DHCP über eine Richtlinie vom Typ *DHCP NetBIOS* festgelegt werden, die im UMC-Modul *Richtlinien* verwaltet wird (siehe auch *Richtlinien* (Seite 77)).

Tab. 11.22: Reiter *Allgemein*

Attribut	Beschreibung
NetBIOS-Nameserver	Hier sind die Namen oder IP-Adressen der NetBIOS-Nameserver (auch bekannt als WINS-Server) einzutragen. Dabei ist darauf zu achten, dass der DHCP-Server diese Namen in IP-Adressen auflösen kann. Die angegebenen Server werden vom Client in der Reihenfolge angesprochen, in der sie in der Auswahlliste erscheinen.
NetBIOS Scope	Der NetBIOS over TCP/IP-Scope für den Client nach der Spezifikation in **RFC 1001**[49] und **RFC 1002**[50]. Bei der Angabe des NetBIOS Scopes ist die Groß- und Kleinschreibung zu beachten.
NetBIOS Node Type	Dieses Auswahlfeld legt den Node Type eines Clients fest. Mögliche Werte sind: • `1 B-node` (Broadcast: kein WINS) • `2 P-node` (Peer: ausschließlich WINS) • `4 M-node` (Mixed: erst Broadcast, dann WINS) • `8 H-node` (Hybrid: erst WINS, dann Broadcast)

Konfiguration der DHCP-Vergabedauer (Lease)

Die Gültigkeit einer vergebenen IP-Adresse - ein sogenanntes DHCP-Lease - kann über eine Richtlinie vom Typ *DHCP Lease-Zeit* festgelegt werden, die im UMC-Modul *Richtlinien* verwaltet wird (siehe auch *Richtlinien* (Seite 77)).

Tab. 11.23: Reiter *Allgemein*

Attribut	Beschreibung
Standard Lease-Zeit	Wenn der Client keine bestimmte Lease-Zeit anfragt, so wird die Standard-Lease-Zeit zugewiesen. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.
Maximale Lease-Zeit	Die maximale Lease-Zeit gibt die längste Zeitspanne an, die für einen Lease vergeben werden kann. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.
Minimale Lease-Zeit	Die minimale Lease-Zeit gibt die kürzeste Zeitspanne an, die ein Lease gültig sein soll. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.

Konfiguration von Bootserver/PXE-Einstellungen

Mit einer *DHCP Boot*-Richtlinie werden Rechnern Konfigurationsparameter für das Booten über BOOTP/PXE zugewiesen. Sie wird im UMC-Modul *Richtlinien* verwaltet (siehe auch *Richtlinien* (Seite 77)).

Tab. 11.24: Reiter *Boot*

Attribut	Beschreibung
Boot-Server	In diesem Eingabefeld ist die IP-Adresse oder der FQDN des PXE-Boot-Servers einzutragen, von dem der Client die Boot-Datei laden soll. Wird in diesem Eingabefeld kein Wert eingetragen, bootet der Client von dem DHCP-Server, von dem er seine IP-Adresse bezieht.
Boot-Dateiname	Hier ist der Pfad zur Boot-Datei einzutragen. Der Pfad muss relativ zum Basisverzeichnis des TFTP-Dienstes (`/var/lib/univention-client-boot/`) angegeben werden.

[49] https://datatracker.ietf.org/doc/html/rfc1001.html
[50] https://datatracker.ietf.org/doc/html/rfc1002.html

Weitere DHCP-Richtlinien

Einige weitere DHCP-Richtlinien stehen zur Verfügung, sind aber nur für Sonderfälle nötig.

DNS Aktualisierung
DNS Aktualisierung erlaubt die Konfiguration von dynamischen DNS-Aktualisierungen. Diese können bislang noch nicht gegen einen LDAP-basierten DNS-Dienst durchgeführt werden, wie er von UCS bereitgestellt wird.

DHCP Erlauben/Verbieten
DHCP Erlauben/Verbieten erlaubt die Konfiguration verschiedener Optionen, die kontrollieren was für DHCP-Clients erlaubt ist. Diese sind nur in Ausnahmefällen nötig.

DHCP Verschiedenes
DHCP Verschiedenes erlaubt die Konfiguration verschiedener Optionen, die nur in Ausnahmefällen nötig sind.

11.4 Paketfilter mit Univention Firewall

Die Univention Firewall integriert einen Paketfilter auf Basis von **`iptables`** in Univention Corporate Server.

Dies ermöglicht die gezielte Filterung unerwünschter Dienste, die Absicherung von Rechnern während Installationsarbeiten, und stellt die Basis für komplexere Szenarien wie Firewalls oder Application Level Gateways bereit. Univention Firewall ist standardmäßig auf allen Univention Corporate Server-Installationen enthalten.

In der Grundeinstellung werden eingehende Pakete für alle Ports blockiert/abgelehnt. Jedes UCS-Paket bringt Regeln mit, die die von dem Paket benötigten Ports wieder freigeben.

Die Konfiguration erfolgt im Wesentlichen über Univention Configuration Registry-Variablen. Die Definition von solchen Paketfilter-Regeln ist in *Univention Developer Reference* [3] dokumentiert.

Darüber hinaus werden die im Verzeichnis `/etc/security/packetfilter.d/` liegenden Konfigurationsskripte in alphabetischer Reihenfolge ausgeführt. Standardmäßig sind alle Skripte mit zwei führenden Ziffern benannt, so dass eine einfache Festlegung der Reihenfolge möglich ist. Die Skripte müssen als ausführbar markiert sein.

Nach Änderungen der Paketfilter-Einstellungen muss der Dienst **`univention-firewall`** neu gestartet werden.

Die Univention Firewall kann durch Setzen der Univention Configuration Registry Variable *`security/packetfilter/disabled`* (Seite 317) auf `true` deaktiviert werden

11.5 Web-Proxy für Caching und Policy Management/Virenscan

Die Proxy-Integration ermöglicht die Verwendung eines Web-Caches zur Verbesserung der Performance und Kontrolle des Datenverkehrs. Sie basiert auf dem bewährten Proxy-Server Squid und unterstützt die Protokolle HTTP, FTP und HTTPS.

Ein Proxy-Server nimmt Anfragen nach Internetinhalten entgegen und prüft, ob diese Inhalte bereits in einem lokalen Cache vorhanden sind. Ist dies der Fall, werden die angefragten Daten aus dem lokalen Cache bereitgestellt. Sind die Daten noch nicht vorhanden, werden die Inhalte vom jeweiligen Webserver abgerufen und in den lokalen Cache eingefügt. Hierdurch können die Antwortzeiten für die Anwender sowie das Transfervolumen über den Internetzugang verringert werden.

Einige weiterführende Funktionen der Proxy-Dienste - wie etwa die Kaskadierung von Proxy-Servern - werden in *Extended IP and network management documentation* [14] beschrieben.

11.5.1 Installation

Squid kann mit der Applikation **Proxyserver / Webcache (Squid)** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **univention-squid** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

Der Dienst wird mit für den Betrieb ausreichenden Standardeinstellungen konfiguriert, sodass eine sofortige Verwendung möglich ist. Der Port, auf dem der Dienst erreichbar ist, kann nach eigenen Wünschen konfiguriert werden (siehe *Zugriffsport* (Seite 238)), voreingestellt ist Port `3128`.

Werden Änderungen an der Konfiguration vorgenommen, muss Squid neu gestartet werden. Dies kann entweder über das UMC-Modul *Systemdienste* oder auf der Kommandozeile erfolgen:

```
$ systemctl restart squid
```

Neben den in diesem Dokument beschriebenen Konfigurationsmöglichkeiten über Univention Configuration Registry können in der Datei `/etc/squid/local.conf` auch beliebige weitere Squid-Optionen gesetzt werden.

11.5.2 Caching von Webseiten

Squid ist ein *Caching proxy*, d.h. zuvor schon einmal angefragte Inhalten können aus einem Cache zur Verfügung gestellt werden ohne erneut vom jeweiligen Webserver geladen zu werden. Dies reduziert das Datenaufkommen über die Internetanbindung und kann zu einer schnelleren Beantwortung von HTTP-Anfragen führen.

In manchen Umgebungen ist diese Caching-Funktionalität allerdings nicht notwendig oder muss bei kaskadierten Proxys nicht bei allen aktiviert sein. Für diese Szenarien kann die Caching-Funktion des Squid mit der Univention Configuration Registry Variable *squid/cache* (Seite 318) deaktiviert werden, indem diese auf den Wert `no` gesetzt wird. Anschließend muss Squid neu gestartet werden.

11.5.3 Protokollierung von Zugriffen

Sämtliche Zugriffe, die über den Proxy-Server vorgenommen werden, werden in der Logdatei `/var/log/squid/access.log` erfasst. Anhand dieser Logdatei ist es möglich, nachzuvollziehen auf welche Webseiten zugegriffen wurde.

11.5.4 Einschränkung des Zugriffs auf erlaubte Netzwerke

Standardmäßig darf nur aus lokalen Netzwerken auf den Proxy-Server zugegriffen werden. Ist z.B. an dem Rechner, auf dem Squid installiert wurde, ein Netzwerkinterface mit der Adresse `192.0.2.10` und der Netzmaske `255.255.255.0` vorhanden, dürfen nur Rechner aus dem Netzwerk `192.0.2.0/24` auf den Proxy-Server zugreifen. Weitere Netzwerke können über die Univention Configuration Registry Variable *squid/allowfrom* (Seite 318) angegeben werden. Dabei muss die CIDR-Notation verwendet werden, mehrere Netzwerke sind durch Leerzeichen zu trennen.

Beispiel:

```
$ univention-config-registry set squid/allowfrom="192.0.2.0/24 192.0.3.0/24"
```

Nach einem Neustart von Squid ist jetzt der Zugriff aus den Netzwerken `192.0.2.0/24` und `192.0.2.0/24` erlaubt. Durch Angabe von `all` kann der Zugriff auch aus allen Netzen erlaubt werden.

11.5.5 Konfiguration der verwendeten Ports

Zugriffsport

Standardmäßig ist der Web-Proxy über den Port `3128` erreichbar. Ist ein anderer Port gewünscht, kann dieser über die Univention Configuration Registry Variable *squid/httpport* (Seite 318) konfiguriert werden. Bei Verwendung von Univention Firewall muss zusätzlich die Paketfilterkonfiguration angepasst werden.

Erlaubte Ports

In der Standardkonfiguration leitet Squid nur Anfragen von Clients weiter, die an die Netzwerkports 80 (HTTP), 443 (HTTPS) oder 21 (FTP) gerichtet werden. Die Liste der erlaubten Ports kann über die Univention Configuration Registry Variable *squid/webports* (Seite 318) geändert werden, mehrere Angaben sind dabei durch Leerzeichen zu trennen.

Beispiel:

```
$ univention-config-registry set squid/webports="80 443"
```

Durch diese Einstellung wird nur noch der Zugriff auf die Ports 80 und 443 (HTTP und HTTPS) erlaubt.

11.5.6 Benutzer-Authentifizierung am Proxy

Oftmals ist es notwendig, dass nur bestimmte Benutzer Zugriff auf Webseiten erhalten sollen. Squid ermöglicht die benutzerbezogene Zugriffsregelung über Gruppenmitgliedschaften. Um eine Überprüfung der Gruppenmitgliedschaft zu ermöglichen, ist es hierbei erforderlich, dass eine Anmeldung des Benutzers am Proxy-Server durchgeführt wird.

Vorsicht: Um zur verhindern, dass nicht autorisierte Benutzer trotzdem Webseiten abrufen können, sind weitere Maßnahmen erforderlich, damit diese Benutzer nicht am Proxy-Server vorbei auf das Internet zugreifen können. Dies kann z.B. erreicht werden, in dem in der Firewall alle HTTP-Anfragen mit Ausnahme des Proxys unterbunden werden.

Proxy-Authentifizierung und die damit erst mögliche Überprüfung der Gruppenzugehörigkeiten muss zuerst aktiviert werden. Dafür werden drei verschiedene Mechanismen angeboten:

LDAP Server Authentifizierung
: Die Authentifizierung erfolgt direkt gegen den LDAP-Server. Dazu müssen die Univention Configuration Registry Variable *squid/basicauth* (Seite 318) auf `yes` gesetzt und Squid neu gestartet werden.

NTLM Authentifizierung
: Die Authentifizierung wird über die NTLM-Schnittstelle durchgeführt. Benutzer, die an einem Windows-Client angemeldet sind, müssen dann beim Zugriff auf den Proxy keine weitere Authentifizierung durchführen. Um NTLM-Authentifizierung zu aktivieren, müssen die Univention Configuration Registry Variable *squid/ntlmauth* (Seite 318) auf `yes` gesetzt und Squid neu gestartet werden.

Kerberos Authentifizierung
: Die Authentifizierung erfolgt über Kerberos. Benutzer, die an einem Windows-Client angemeldet sind, der Mitglied einer Samba/AD-Domäne ist, authentifizieren sich am Proxy mit dem Ticket, das sie im Rahmen der Domänenanmeldung erhalten haben. Um Kerberos-Authentifizierung zu aktivieren muss das Paket **univention-squid-kerberos** auf jedem Proxyserver installiert werden. Anschließend müssen die Univention Configuration Registry Variable *squid/krb5auth* (Seite 318) auf `yes` gesetzt und Squid neu gestartet werden.

Bei Verwendung von NTLM-Authentifizierung wird standardmäßig für jede HTTP-Anfrage eine NTLM-Authentifizierung durchgeführt. Wird beispielsweise die Webseite <https://www.univention.de/> aufgerufen, werden neben der eigentlichen HTML-Seite auch weitere Unterseiten und Bilder nachgeladen. Die NTLM-Authentifizierung kann domänenbezogenen zwischengespeichert werden: Wird die Univention Configuration Registry Variable *squid/ntlmauth/keepalive* (Seite 318) auf `yes` gesetzt, wird für nachgelagerte

HTTP-Anfragen derselben Domäne keine weitere NTLM-Authentifizierung durchgeführt. Bei Problemen mit lokalen Benutzerkonten kann es helfen, diese Variable auf `no` zu setzen.

In der Grundeinstellung können alle Benutzer auf den Proxy zugreifen. Mit der Univention Configuration Registry Variable *squid/auth/allowed_groups* (Seite 317) kann der Zugriff auf eine oder mehrere Gruppen beschränkt werden. Bei Angabe mehrerer Gruppen sind diese durch ein Semikolon zu trennen.

11.6 RADIUS

Die **RADIUS** App erhöht die Sicherheit für mit UCS verwaltete IT-Infrastrukturen durch Zugangskontrollen zu WLAN-Netzwerken für Benutzer, Gruppen und Endgeräte über das RADIUS-Protokoll[51]. Die Konfiguration erfolgt über Blacklisten und Whitelisten direkt am Benutzer-, Gruppen- oder Endgeräte-Objekt im UCS Managementsystem. Registrierte Benutzer werden mit ihrem üblichen Domänenpasswort oder alternativ mit einem eigens erzeugten RADIUS-Passwort authentisiert, so dass unter anderem *Bring-Your-Own-Device-Konzepte* ermöglicht werden.

11.6.1 Installation

RADIUS steht über das App Center (siehe *Univention App Center* (Seite 96)) zur Verfügung und kann über das entsprechende UMC-Modul *App Center* installiert werden. Die App kann auf mehreren Systemen installiert werden. Nach der Installation startet die App einen FreeRADIUS[52] Server. *Authenticators* (z.B. *Access Points*) können den Server via RADIUS kontaktieren und Netzwerkzugangsanfragen prüfen.

Die RADIUS App kann auch auf UCS@school Systemen installiert werden. In diesem Fall kann der Zugang an Benutzer oder Gruppen unabhängig von der Internetregel oder Computerraumeinstellungen vergeben werden.

11.6.2 Konfiguration

Erlaubte Benutzer

Standardmäßig hat kein Benutzer Zugang zum Netzwerk. Indem die Checkbox für *Netzwerkzugriff erlaubt* im *RADIUS* Reiter aktiviert wird, erhält der Benutzer Zugriff auf das Netzwerk. Die Checkbox kann auch für Gruppen gesetzt werden, so dass alle Benutzer in der Gruppe Zugang erlangen.

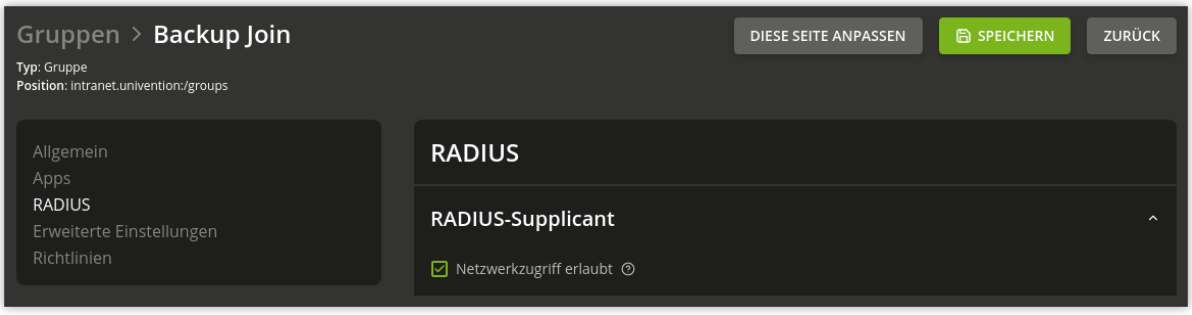


Abb. 11.4: Beispiel für eine Gruppe, die ihren Benutzern Zugang gewährt

[51] https://de.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
[52] https://www.freeradius.org/

Dienst-spezifisches Passwort

Standardmäßig authentifizieren sich die Benutzer mit ihrem Passwort für die Domäne. RADIUS verwendet ein dediziertes Passwort, wenn ein Administrator den Parameter Univention Configuration Registry Variable *radius/use-service-specific-password* (Seite 316) auf `true` setzt. Benutzer können ein spezielles Passwort für die Verwendung von WLAN über die *Self Service App* (Seite 124) anfordern. UCS und die **Self Service** App generieren ein Zufallspasswort für jede Passwortanfrage. Bei Bedarf können die Benutzer jederzeit ein Zufallspasswort erzeugen, wodurch auch das bestehende Passwort ungültig wird.

Um die dienst-spezifische Passwortseite in der **Self Service** App zu aktivieren, muss der Administrator die Univention Configuration Registry Variable `umc/self- service/service-specific-passwords/backend/enabled` auf dem UCS-System, auf dem die **Self Service Backend** App installiert ist, auf den Wert `true` setzen.

UCS ermöglicht die Konfiguration der Passwortqualität für die automatisch generierten und dienst-spezifischen Passwörter durch die folgenden Univention Configuration Registry Variablen. Eine Beschreibung finden Sie in den Verweisen auf die jeweiligen generischen Passwortqualitätseinstellungen.

Tab. 11.25: RADIUS Passwortqualitätsparameter

RADIUS Passwortqualitätsparameter	Allgemeiner Qualitätsparameter für Passwörter
`password/radius/quality/credit/digits`	*password/quality/credit/digits* (Seite 315)
`password/radius/quality/credit/lower`	*password/quality/credit/lower* (Seite 315)
`password/radius/quality/credit/other`	*password/quality/credit/other* (Seite 315)
`password/radius/quality/credit/upper`	*password/quality/credit/upper* (Seite 315)
`password/radius/quality/forbidden/chars`	*password/quality/forbidden/chars* (Seite 315)
`password/radius/quality/length/min`	*password/quality/length/min* (Seite 315)

Wichtig: Die Einstellungen in den `password/quality/**` Univention Configuration Registry Variablen haben keinen Einfluss auf das dienst-spezifische Passwort.

Um die Passwortqualität zu konfigurieren, wählen Sie von den folgenden Reitern das Szenario aus, das Ihrer Umgebung entspricht, in der Sie die **RADIUS** App installiert haben.

Führen Sie die folgenden Schritte aus, um die Passwortqualität zu konfigurieren.

Voraussetzung
Sie haben die **RADIUS** App auf dem Primary Directory Node installiert.

1. Die verfügbaren Qualitätsparameter für Passwörter finden Sie entweder in Tab. 11.25 oder in Ihrem System.

   Öffnen Sie **auf dem Primary Directory Node** die Befehlszeile und sehen Sie die verfügbaren Qualitätsparameter für Passwörter nach:

   ```
   $ ucr search password/radius/quality
   ```

2. Wählen Sie den Parameter, den Sie ändern möchten, und stellen Sie die entsprechende Univention Configuration Registry Variable ein, z. B. die minimale Passwortlänge.

   ```
   $ ucr set password/radius/quality/length/min=32
   ```

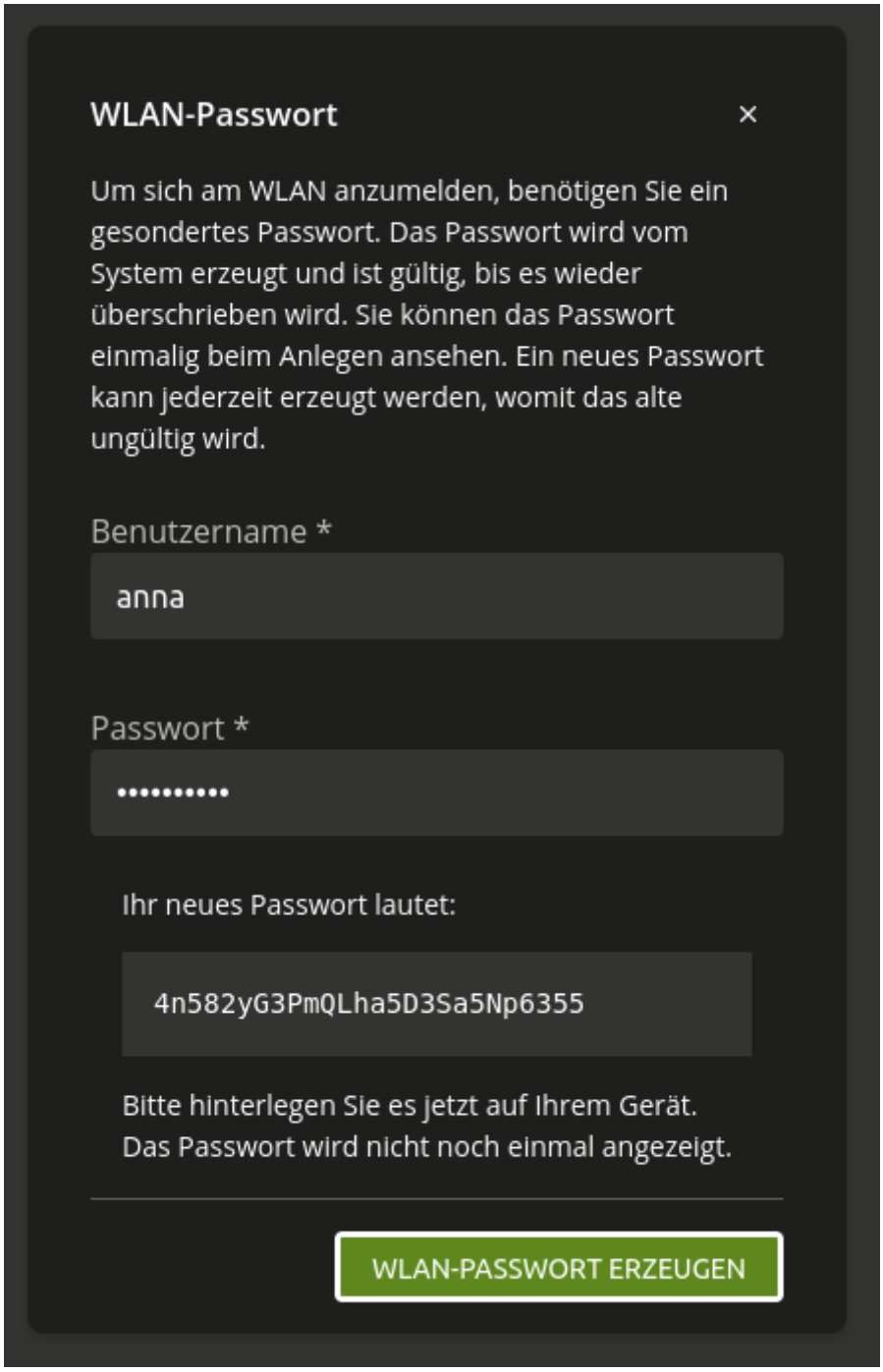


Abb. 11.5: Seite im Self Service, um ein RADIUS-spezifisches Passwort zu bekommen

Führen Sie die folgenden Schritte aus, um die Passwortqualität zu konfigurieren.

Voraussetzung
Sie haben die Anwendung **RADIUS** auf einem **anderen** UCS System installiert, als den Primary Directory Node.

1. Die verfügbaren Qualitätsparameter für Passwörter finden Sie entweder in Tab. 11.25 oder in Ihrem System.

   Auf dem UCS-System, auf dem die **RADIUS** App installiert ist, öffnen Sie die Befehlszeile und sehen Sie die verfügbaren Qualitätsparameter für Passwörter nach:

   ```
   $ ucr search password/radius/quality
   ```

2. Wählen Sie den Parameter, den Sie ändern möchten, und setzen Sie die entsprechende Univention Configuration Registry Variable, z. B. die minimale Passwortlänge. Öffnen Sie auf dem Primary Directory Node die Befehlszeile und führen Sie den folgenden Befehl aus:

   ```
   $ ucr set password/radius/quality/length/min=32
   ```

3. Unabhängig vom Szenario müssen Sie schließlich die *UDM HTTP REST API* auf dem Primary Directory Node neu starten. Öffnen Sie die Befehlszeile und führen Sie den folgenden Befehl aus.

   ```
   $ systemctl restart univention-directory-manager-rest.service
   ```

MAC-Adressfilter

Standardmäßig ist allen Geräten der Zugang zum Netzwerk erlaubt, vorausgesetzt der verwendete Benutzer hat Zugriff. Der Netzwerkzugriff kann auch auf spezifische Geräte begrenzt werden. Das kann durch Setzen der Univention Configuration Registry Variable *radius/mac/whitelisting* (Seite 316) auf `true` erreicht werden. Sobald aktiviert, wird das Geräteobjekt beim Zugriff des Geräts auf das Netzwerk über das LDAP-Attribut `macAddress` abgerufen und dem entsprechenden Geräteobjekt muss der Zugang zum Netzwerk auch erlaubt sein (entweder direkt oder über eine der Gruppen).

MAC Authentication Bypass für Computerobjekte

MAC Authentication Bypass (MAB) ist ein proprietärer Fallback-Modus zu 802.1X für Geräte, die keine 802.1X-Authentifizierung unterstützen, wie Netzwerkdrucker oder drahtlose Telefone. MAB ist eine Option, die es solchen Geräten ermöglicht, sich mit ihrer MAC-Adresse als Benutzernamen beim Netzwerk zu authentifizieren.

Dieser Abschnitt beschreibt, wie Sie die MAC-Adresse eines Geräts zur Authentifizierung verwenden und ihm über MAB ein VLAN der entsprechenden Netzwerkinfrastruktur zuweisen. Um MAC Authentication Bypass zu aktivieren, setzen Sie die Univention Configuration Registry Variable *freeradius/conf/allow-mac-address-authentication* (Seite 306) auf `true`.

Wichtig: Geräte, die sich mit MAB authentifizieren, ignorieren die Netzwerkzugangseinstellungen:

- Univention Configuration Registry Variable *radius/mac/whitelisting* (Seite 316)
- Die Checkbox *Netzwerkzugriff zulassen* beim Computerobjekt und in der Gruppeneinstellung

---

Warnung: Angreifer können MAC-Adressen ausspionieren. Betrachten Sie jeden Anschluss als gefährdet, an dem Ihr Switch die Verwendung von MAB zulässt. Vergewissern Sie sich, dass Sie geeignete Maßnahmen ergriffen haben, um Ihr Netzwerk weiterhin sicher zu halten.

Um einem Computer die VLAN-ID zuzuweisen, müssen Sie ihn zur Gruppe des Computerobjekts hinzufügen, dass die entsprechende VLAN ID hat. Gehen Sie im UCS-Managementsystem wie folgt vor:

1. Öffnen Sie *Geräte* ‣ *Computer*.

2. Klicken Sie das Computerobjekt, das Sie bearbeiten möchten.
3. Gehen Sie zu *Erweiterte Einstellungen* ‣ *Gruppen*.
4. Um eine Gruppe mit VLAN-IDs hinzuzufügen, klicken Sie auf *ADD*, wählen Sie `Virtual LAN ID` aus der Dropdown-Liste *Objekteigenschaft* und aktivieren Sie die entsprechende Gruppe, um sie hinzuzufügen.
5. Um zu speichern, klicken Sie auf *HINZUFÜGEN* im *Objekte hinzufügen* Dialog und *SAVE* in *Erweiterte Einstellungen*.

Um die VLAN-ID einer Benutzergruppe zuzuweisen, müssen Sie sie zu den Benutzergruppeneinstellungen hinzufügen. Führen Sie im UCS-Managementsystem die folgenden Schritte aus:

1. Öffnen Sie *Benutzer* ‣ *Gruppen*.
2. Klicken Sie die Benutzergruppe zum Bearbeiten oder erstellen Sie eine neue Benutzergruppe.
3. Gehen Sie zu *RADIUS*.
4. Geben Sie die VLAN ID as Zahl in das Feld *Virtual LAN ID*.
5. Zum Speichern, klicken Sie *SPEICHERN*.

Wenn einem Computerobjekt mehrere Gruppen mit VLAN-IDs zugeordnet sind, wählt UCS die VLAN-ID mit der niedrigsten Nummer aus und weist sie zu. Um eine Standard VLAN-ID zu konfigurieren, setzen Sie diese als Wert in die Univention Configuration Registry Variable *freeradius/vlan-id* (Seite 306).

Nachdem Sie die Konfiguration abgeschlossen haben, gibt der Radius-Server die zugewiesene VLAN-ID an Anfragen mit der angegebenen MAC-Adresse zurück.

UCS speichert die MAC-Adresse im LDAP-Verzeichnis als Zeichenkette in Kleinbuchstaben mit dem Doppelpunkt (`:`) als Trennzeichen, zum Beispiel `00:00:5e:00:53:00`.

Neu in Version 5.0-6-erratum-1011: Mit UCS 5.0 erratum 1011[53] kann der Radius-Server mit verschiedenen Formaten der MAC Adresse für Benutzernamen umgehen, wenn MAB verwendet wird.

Geräte, die MAB verwenden, benutzen ihre MAC-Adresse als Benutzernamen und sie können unterschiedliche Formate dafür verwenden. Der Radius-Server unterstützt verschiedene Formate, die Groß- und Kleinschreibung unterscheiden. In der folgenden Liste sind die getesteten Formate aufgeführt:

- `XX:XX:XX:XX:XX:XX`
- `XX-XX-XX-XX-XX-XX`
- `XX.XX.XX.XX.XX.XX`
- `XXXX.XXXX.XXXX`
- `XXXXXXXXXXXX`

Bemerkung: Für nicht-standardisierte Formate können Sie einen regulären Ausdruck in der Univention Configuration Registry Variable *freeradius/conf/mac-addr-regexp* (Seite 306) konfigurieren, der mit Ihrem benutzerdefinierten MAC-Adressformat zusammen passt.

Je nach regulärem Ausdruck kann es vorkommen, dass die zuvor aufgeführten Formate nicht mehr funktionieren.

Wichtig: Alle Geräte, die MAB verwenden, müssen dasselbe Passwort haben, da *dienstspezifische Passwörter* (Seite 240) nicht funktionieren, und der Switch muss das Passwort kennen. Sie können nur ein Gerätepasswort im Switch konfigurieren. Sie können Ihr eigenes Passwort für die Geräte mit MAB erstellen, zum Beispiel `mab request format attribute 2 password1`.

[53] https://errata.software-univention.de/#/?erratum=5.0x1011

Wenn die Netzwerkinfrastruktur ein anderes Format vorsieht, können Sie das Format häufig neu konfigurieren. Für Cisco-Switches können Sie zum Beispiel `mab request format attribute 1 groupize 2 separator : lowercase` verwenden, wie in Configurable MAB Username and Password[54] beschrieben.

Access Points verwalten

Alle *Access Points* (Netzwerkzugangspunkte) müssen dem RADIUS-Server bekannt sein. Ein *Access Point* lässt sich entweder pro RADIUS-Server über die Datei `/etc/freeradius/3.0/clients.conf` konfigurieren oder domänenweit über das UMC-Modul *Rechner*. Für jeden *Access Point* sollte ein zufälliges, gemeinsames Geheimnis erzeugt werden (Zum Beispiel über den Befehl **`makepasswd`**.). Der Name kann frei gewählt werden.

Beispiel für einen Eintrag eines Access Points in der `clients.conf` Datei:

```
client AP01 {
    secret = a9RPAeVG
    ipaddr = 192.0.2.101
}
```

Um *Access Points* über das UMC-Modul *Rechner* zu verwalten muss ein Rechnerobjekt erstellt oder ausgewählt werden und die Option *RADIUS-Authenticator* (*Setzen der RADIUS-Option* (Seite 244)) aktiviert werden. Für einen *Access Point* bietet sich ein *IP-Client* als Rechnerobjekt an. Im *RADIUS*-Reiter des Objekts lassen sich nach dem Hinzufügen der Option die Eigenschaften des *Access Points* festlegen (*RADIUS-Authenticator Optionen* (Seite 245)). Es müssen mindestens die IP-Adresse am Rechnerobjekt und ein gemeinsamer, geheimer Schlüssel gesetzt sein. Die Eigenschaften *NAS-Type* und Virtueller Server müssen in der Regel nicht verändert werden.

Access Points, welche über UMC-Modul *Rechner* konfiguriert sind, sind anschließend allen RADIUS-Servern in der Domäne bekannt. Dabei werden die *Access Points* über den Univention Directory Listener in die Datei `/etc/freeradius/3.0/clients.univention.conf` geschrieben und der RADIUS-Server neu gestartet. Um Änderungen zusammenzufassen, geschieht dies verzögert (etwa 15 Sekunden). Neue *Access Points* haben erst nach diesem Neustart Zugriff auf den RADIUS-Server.

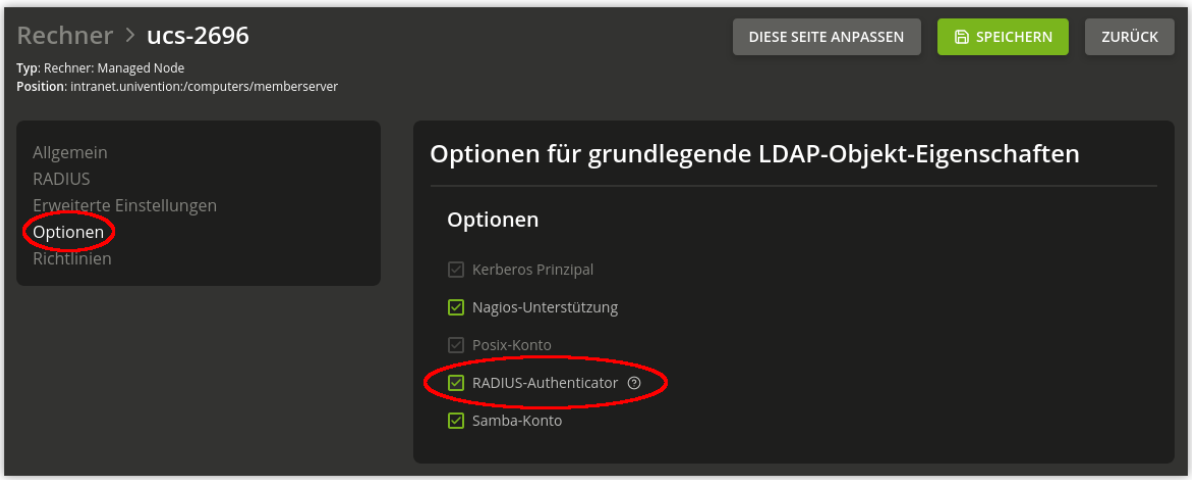


Abb. 11.6: Setzen der RADIUS-Option

[54] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-e/sec-usr-aaa-15-e-book/sec-usr-config-mab-usrname-pwd.html

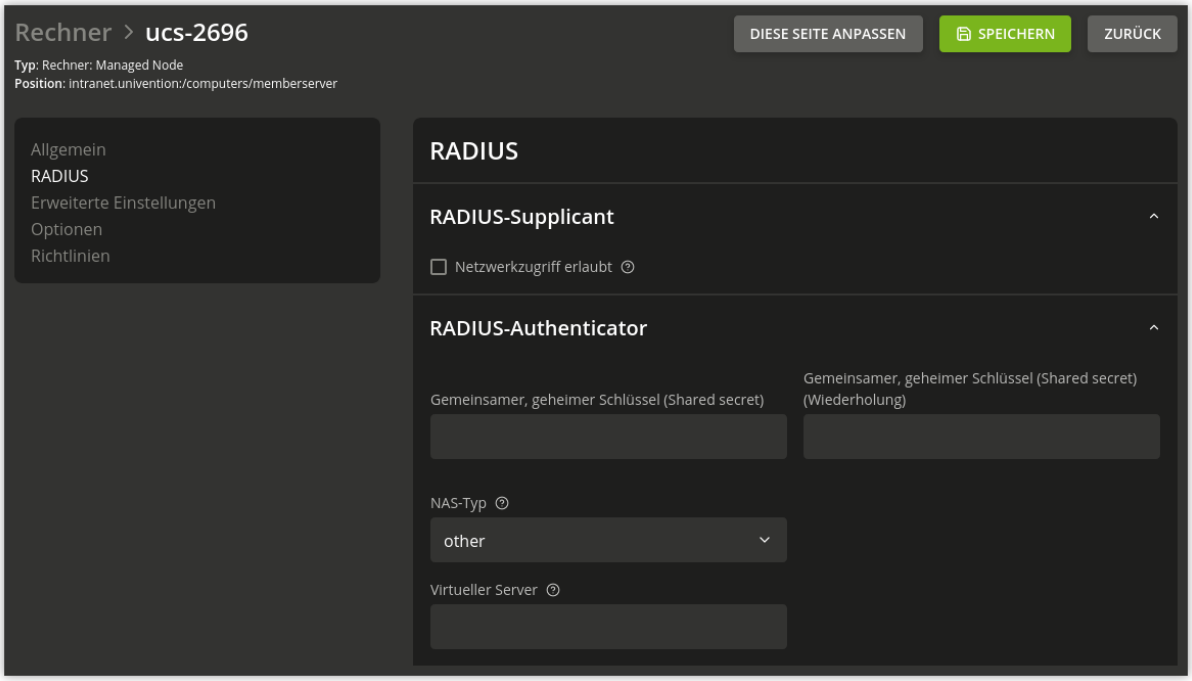


Abb. 11.7: *RADIUS-Authenticator* Optionen

Konfiguration von Access Point und Client

Die *Access Points* müssen so konfiguriert sein, dass sie 802.1x („WPA Enterprise“) Authentisierung verwenden. Außerdem sollte die *RADIUS Server* Adresse auf die Adresse des Servers gesetzt sein, auf dem die **RADIUS**-App installiert ist. Das Passwort muss auf den Wert des des `secret` aus dem Eintrag in der `clients.conf` für den Access Point gesetzt sein.

WLAN Clients müssen so konfiguriert sein, dass sie *WPA* mit *PEAP* und *MSCHAPv2* für die Authentisierung verwenden.

VLAN IDs

Virtual Local Area Networks (VLANs) können verwendet werden, um den Datenverkehr der Benutzer auf der Netzwerkebene zu trennen. UCS kann so konfiguriert werden, dass es eine VLAN-ID in der Radius-Antwort des Radius-Authentifizierungsprozesses gemäß **RFC 3580 / IEEE 802.1X**[55] zurück gibt. Weitere Informationen finden Sie in *Konfiguration VLAN* (Seite 158).

Die VLAN-ID für einen Benutzer kann konfiguriert werden, indem der Benutzer einer Gruppe mit einer VLAN-ID zugewiesen wird.

Eine Standard VLAN-ID kann in der Univention Configuration Registry Variable *freeradius/vlan-id* (Seite 306) konfiguriert werden. Diese Standard VLAN-ID wird zurückgegeben, wenn der Benutzer nicht Mitglied einer Gruppe mit einer VLAN-ID ist. Die Radius Antwort wird keine VLAN-ID enthalten, wenn der Benutzer nicht Mitglied einer Gruppe mit VLAN-ID ist und keine Standard VLAN-ID definiert ist.

[55] https://datatracker.ietf.org/doc/html/rfc3580.html

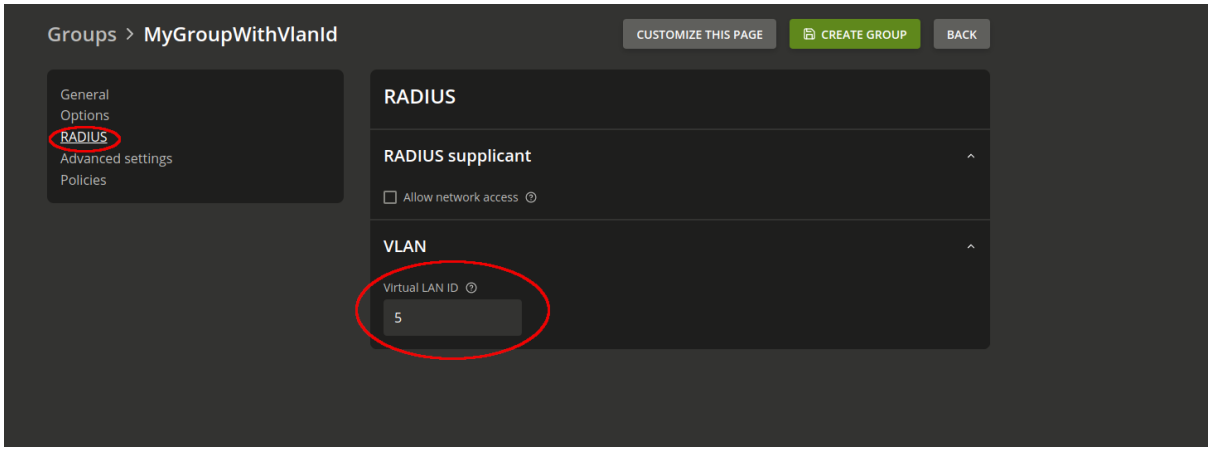


Abb. 11.8: Zuweisung VLAN ID zu einer Benutzergruppe

11.6.3 Fehlersuche

Die **RADIUS**-App verfügt über eine Logdatei unter `/var/log/univention/radius_ntlm_auth.log`. Die Ausführlichkeit der Logmeldungen lässt sich über die Univention Configuration Registry Variable *freeradius/auth/helper/ntlm/debug* (Seite 306) steuern. Der **FreeRADIUS-Server** loggt nach `/var/log/freeradius/radius.log`.

Das Werkzeug **univention-radius-check-access** kann zur Untersuchung der aktuellen Zugangsregeln für einen bestimmten Benutzer und/oder eine MAC-Adresse verwendet werden. Es kann als Benutzer root auf dem Server ausgeführt werden, wo das Paket **univention-radius** installiert ist:

```
root@primary211:~# univention-radius-check-access --username=stefan --station-id␣
↪none
DENY 'uid=stefan,cn=users,dc=ucs,dc=example'
'uid=stefan,cn=users,dc=ucs,dc=example'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=example'
Thus access is DENIED.
```

```
root@primary211:~# univention-radius-check-access --username=janek --station-id␣
↪none
DENY 'uid=janek,cn=users,dc=ucs,dc=example'
'uid=janek,cn=users,dc=ucs,dc=example'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> ALLOW 'cn=Network Access,cn=groups,dc=ucs,dc=example'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> 'cn=Network Access,cn=groups,dc=ucs,dc=example'
Thus access is ALLOWED.
root@primary211:~#
```

Das Werkzeug gibt eine detaillierte Erläuterung und setzt den Rückgabewert abhängig vom Ergebnis der Zugangsprüfung (`0` für *Zugang gestattet*, `1` für *Zugang verweigert*).

KAPITEL 12

Verwaltung von Freigaben

UCS unterstützt die zentrale Verwaltung von Verzeichnisfreigaben. Eine im UMC-Modul *Freigaben* registrierte Freigabe wird im Rahmen der UCS-Domänenreplikation auf beliebigen Serversystemen der UCS-Domäne angelegt.

Die Bereitstellung für die zugreifenden Clients kann über CIFS (unterstützt von Windows/Linux-Clients) und/oder NFS (vorrangig unterstützt von Linux/Unix) erfolgen. Die im UMC-Modul verwalteten NFS-Freigaben können von Clients sowohl über NFSv3, als auch über NFSv4 eingebunden werden.

Wird eine Verzeichnisfreigabe gelöscht, bleiben die in dem Verzeichnis freigegebenen Daten auf einem Server erhalten.

Um auf einer Freigabe Access Control Lists einzusetzen, muss das unterliegende Linux-Dateisystem POSIX-ACLs unterstützen. In UCS unterstützen die Dateisysteme `ext4` und `XFS` POSIX-ACLs. Die Samba-Konfiguration erlaubt außerdem die Speicherung von DOS-Datei-Attributen in erweiterten Attributen des Unix-Dateisystems. Um erweiterte Attribute zu nutzen, muss die Partition mit der Mount-Option `user_xattr` eingebunden werden.

12.1 Zugriffsrechte auf Daten in Freigaben

Die Verwaltung von Zugriffsrechten auf Dateien erfolgt in UCS anhand von Benutzern und Gruppen. Alle Fileserver der UCS-Domäne greifen über das LDAP-Verzeichnis auf identische Benutzer- und Gruppendaten zu.

Pro Datei werden drei Zugriffsrechte unterschieden:

- Lesen
- Schreiben
- Ausführen

Pro Verzeichnis gelten ebenfalls drei Zugriffsrechte: Lesen, Schreiben und das Recht zu Ausführen von Programm, dass sich hier auf die Berechtigung bezieht, in ein Verzeichnis zu wechseln.

Jede Datei/Verzeichnis wird von einem Benutzer und einer Gruppe besessen. Die drei oben genannten Rechte können jeweils auf den Besitzer, die Besitzer-Gruppe und alle anderen angewendet werden.

setuid
: Ist die *setuid*-Option für eine ausführbare Datei gesetzt, kann diese von Benutzern mit den Rechten des Besitzers oder der Besitzergruppe ausgeführt werden.

setgid
: Wird die Option *setgid* für ein Verzeichnis gesetzt, erben dort angelegte Dateien die Besitzergruppe des Verzeichnisses. Werden weitere Verzeichnisse angelegt, erben diese ebenfalls die Option.

sticky bit
: Ist die Option *sticky bit* für ein Verzeichnis aktiviert, können Dateien in dem Verzeichnis nur von dem Besitzer der Datei oder durch den root-Benutzer gelöscht werden.

Mit Access Control Lists sind noch mächtigere Berechtigungsmodelle möglich. Die Konfiguration von ACLs ist in SDB 1042[56] beschrieben.

Im Unix-Berechtigungsmodell - und somit unter UCS - reicht das Schreibrecht auf eine Datei nicht aus, um die Berechtigungen einer Datei zu verändern. Dies bleibt den Besitzern/der Besitzergruppe einer Datei vorbehalten. Unter Microsoft Windows hingegen verfügen alle Benutzer mit Schreibrechten auch über die Berechtigung, die Berechtigungen anzupassen. Dieses Verhalten kann für CIFS-Freigaben angepasst werden (siehe *Verwaltung von Freigaben über Univention Management Console Modul* (Seite 248)).

Beim Anlegen einer Verzeichnisfreigabe werden nur initiale Besitzer und Zugriffsrechte vergeben. Existiert das Verzeichnis bereits, werden die Berechtigungen des vorhandenen Verzeichnisses angepasst.

Berechtigungsänderungen an einem freigegebenen Verzeichnis, die direkt im Dateisystem vorgenommen wurden, werden nicht an das LDAP-Verzeichnis weitergeleitet. Werden Berechtigungen oder Besitzer im UMC-Modul *Freigaben* bearbeitet, werden die Änderungen im Dateisystem überschrieben. Einstellungen der Freigabewurzel sollten deshalb nur mit dem UMC-Modul gesetzt und bearbeitet werden. Die weitere Anpassung der Zugriffsrechte der unterliegenden Verzeichnisses erfolgt dann von den zugreifenden Clients, z.B. über den Windows-Explorer, oder direkt über Kommandozeilenbefehle auf dem Fileserver.

Die Freigabe *homes* nimmt unter Samba eine Sonderstellung ein. Sie dient der Freigabe der Heimatverzeichnisse der Benutzer. Für jeden Benutzer wird diese Freigabe automatisch in das eigene Heimatverzeichnis umgewandelt. Deswegen ignoriert Samba die zugewiesenen Rechte der Freigabe und verwendet die Rechte des jeweiligen Heimatverzeichnisses.

12.2 Verwaltung von Freigaben über Univention Management Console Modul

Verzeichnisfreigaben werden im UMC-Modul *Freigaben* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)).

Beim Hinzufügen/Bearbeiten/Entfernen einer Freigabe wird diese in die Datei `/etc/exports`, und/oder in die Samba-Konfigurationsdatei eingetragen/modifiziert oder entfernt.

[56] https://help.univention.com/c/knowledge-base/supported/48

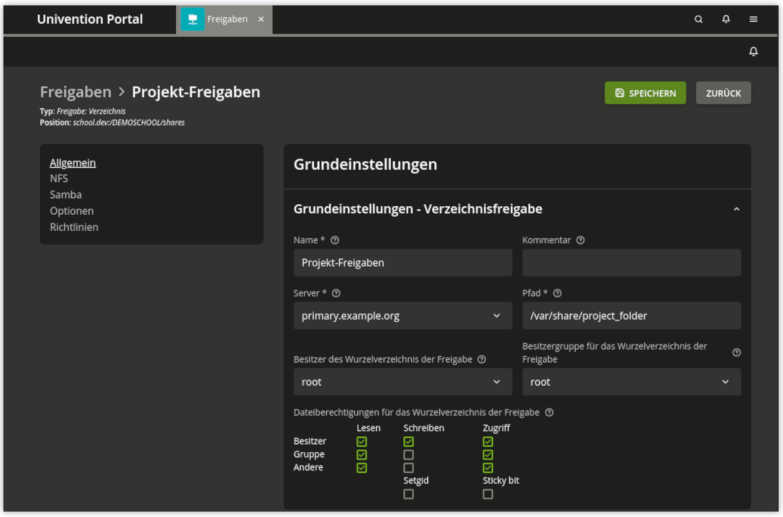


Abb. 12.1: Anlegen einer Freigabe im UMC-Modul *Freigaben*

12.2.1 Freigaben UMC Modul - Reiter Allgemein

Tab. 12.1: Reiter *Allgemein*

Attribut	Beschreibung
Name	Hier ist der Name der Freigabe einzutragen. Der Name darf nur aus Buchstaben, Ziffern, Punkten oder Leerzeichen bestehen und muss mit einem Buchstaben oder einer Ziffer beginnen und enden.
Kommentar	Eine frei wählbare Beschreibung für diese Freigabe. Diese wird auch im Dateibrowser von Windows angezeigt.
Server	Der Server, auf dem die Freigabe liegt. Zur Wahl stehen alle im LDAP-Verzeichnis für die Domäne eingetragenen Rechner vom Typ Primary/Backup/Replica Directory Node und Managed Node, die in einer DNS Forward Lookup Zone im LDAP-Verzeichnis eingetragen sind.
Pfad	Der absolute Pfad des freizugebenden Verzeichnisses ohne Anführungszeichen (auch wenn der Pfad z.B. Leerzeichen enthält). Wenn das Verzeichnis noch nicht existiert, wird es automatisch auf dem ausgewählten Server angelegt. Ist die Univention Configuration Registry Variable `listener/shares/rename` (Seite 309) auf `yes` gesetzt, wird bei der Änderung des Pfads der Inhalt eines bestehenden Verzeichnisses verschoben. Auf und unterhalb von `/proc`, `/tmp`, `/root`, `/dev` und `/sys` können keine Freigaben angelegt oder dorthin verschoben werden.
Besitzer des Wurzelverzeichnis der Freigabe	Der Benutzer, dem das Wurzelverzeichnis der Freigabe gehören soll, siehe *Zugriffsrechte auf Daten in Freigaben* (Seite 247).
Besitzergruppe für das Wurzelverzeichnis der Freigabe	Die Gruppe, der das Wurzelverzeichnis der Freigabe gehören soll, siehe *Zugriffsrechte auf Daten in Freigaben* (Seite 247).
Dateiberechtigungen für das Wurzelverzeichnis der Freigabe	Die Lese-, Schreib- und Zugriffsrechte für das Wurzelverzeichnis der Freigabe, siehe *Zugriffsrechte auf Daten in Freigaben* (Seite 247).

12.2.2 Freigaben UMC Modul - Reiter NFS

Freigaben UMC Modul - NFS Gruppe

Tab. 12.2: *NFS* Gruppe

Attribut	Beschreibung
NFS-Schreibzugriff	Erlaubt schreibenden NFS-Zugriff auf diese Freigabe, ansonsten kann die Freigabe nur lesend verwendet werden.
Subtree-Überprüfung	Wird nur ein Unterverzeichnis eines Dateisystems exportiert, muss der NFS-Server bei jedem Zugriff überprüfen, ob die zugegriffene Datei auf dem exportierten Dateisystem und in dem exportierten Pfad liegt. Für diese Prüfung werden Pfad-Informationen an den Client übergeben. Die Aktivierung dieser Funktion kann zu Problemen führen, wenn eine auf dem Client geöffnete Datei umbenannt wird.
User-ID für Root-Benutzer ändern (Root-Squashing)	Die Identifikation von Nutzern im NFS-Standardverfahren erfolgt über User-IDs. Um zu verhindern, dass ein lokaler Root-Nutzer auf fremden Freigaben ebenfalls mit Root-Rechten arbeitet, kann der Root-Zugriff umgelenkt werden. Ist diese Option aktiviert, erfolgen Root-Zugriffe als Benutzer `nobody`. Die standardmäßig leere lokale Gruppe `staff` verfügt über Privilegien, die `root`-Rechten recht nahe kommen, wird aber von der Weiterleitung nicht berücksichtigt. Dies sollte bei der Aufnahme von Nutzern in diese Gruppe berücksichtigt werden.
NFS-Synchronisation	Der Synchronisationsmodus für die Freigabe. Mit der Einstellung `sync` werden Daten direkt auf das unterliegende Speichermedium geschrieben. Die gegenteilige Einstellung - `async` - kann die Performance verbessern, birgt aber auch das Risiko von Datenverlusten wenn der Server ohne kontrolliertes Herunterfahren abgeschaltet wird.
Zugriff nur für diese Rechner, IP-Adressen oder Netze erlauben	Standardmäßig wird allen Rechnern der Zugriff auf eine Freigabe erlaubt. In die Auswahlliste können Rechnernamen und IP-Adressen aufgenommen werden, auf die dann der Zugriff auf die Freigabe beschränkt wird. Hier ließe sich etwa der Zugriff auf eine Freigabe mit Maildaten auf den Mailserver der Domäne einschränken.

Freigaben UMC Modul - Gruppe Erweiterte NFS-Einstellungen

Tab. 12.3: Gruppe *Erweiterte NFS-Einstellungen*

Attribut	Beschreibung
Erweiterte NFS-Einstellungen für Freigaben	Neben den in der Gruppe *NFS* konfigurierbaren Eigenschaften einer NFS-Freigabe ermöglicht diese Einstellung beliebige weitere NFS-Einstellungen an einer Freigabe zu setzen. Eine Liste der verfügbaren Optionen kann mit dem Befehl **`man 5 exports`** abgerufen werden. Doppelt angegebene Konfigurationsoptionen werden nicht überprüft.

Vorsicht: Das Setzen erweiterter NFS-Einstellungen ist nur in Sonderfällen nötig. Die Optionen sollten vor dem Setzen gründlich geprüft werden, da sie unter Umständen sicherheitsrelevante Auswirkungen haben können.

12.2.3 Freigaben UMC Modul - Reiter Samba

Freigaben UMC Modul - Gruppe Samba

Tab. 12.4: Reiter *Samba*

Attribut	Beschreibung
Windows-Name	Der NetBIOS-Name der Freigabe. Unter diesem Namen wird die Freigabe auf Windows-Rechnern in der Netzwerkumgebung angezeigt. Das UMC-Modul übernimmt beim Hinzufügen einer Verzeichnisfreigabe als Vorgabe den Namen, der auf der Karteikarte *Allgemein* im Feld *Name* eingetragen ist.
Freigabe in der Windows-Netzwerkumgebu anzeigen	Konfiguriert, ob diese Freigabe auf Windows-Rechnern in der Netzwerkumgebung angezeigt werden soll.
Anonymen Nur-Lese-Zugriff mit Gastbenutzer erlauben	Erlaubt den Zugriff auf diese Freigabe ohne Passwortabfrage. Alle Zugriffe werden dabei über einen gemeinsamen Gast-Nutzer `nobody` durchgeführt.
Freigabe als MSDFS-Wurzel freigeben	Diese Option ist in *Unterstützung von MSDFS* (Seite 255) dokumentiert.
Verstecke nicht lesbare Dateien und Verzeichnisse	Wenn diese Option aktiviert ist, werden Dateien, die anhand der Dateirechte für einen Benutzer nicht lesbar sind, für diesen nicht angezeigt.

Freigaben UMC Modul - Gruppe Samba-Rechte

Tab. 12.5: Gruppe *Samba-Rechte*

Attribut	Beschreibung
Benutzer mit Schreibrechten dürfen die Berechtigungen verändern	Wird diese Option aktiviert, erhalten alle Benutzer mit Schreibrechten auf eine Datei auch die Möglichkeiten Berechtigungen, ACL-Einträge und Dateibesitzrechte zu ändern, siehe *Zugriffsrechte auf Daten in Freigaben* (Seite 247).
Erzwungener Benutzer	Der Benutzername, mit dessen Namen, Rechten und primärer Gruppe alle Dateioperationen zugreifender Benutzer ausgeführt werden sollen. Der Benutzername wird erst verwendet, nachdem der Benutzer mit seinem tatsächlichen Benutzernamen und gültigem Passwort eine Verbindung zur Samba-Freigabe aufgebaut hat. Ein gemeinsamer Benutzername ist nützlich, um Dateien gemeinsam zu benutzen, kann bei falscher Anwendung aber Sicherheitsprobleme verursachen.
Erzwungene Gruppe	Eine Gruppe, die alle Benutzer, die sich mit dieser Freigabe verbinden, als primäre Gruppe verwenden sollen. Dadurch gelten die Rechte dieser Gruppe als Gruppenrechte für alle diese Benutzer. Eine hier eingetragene Gruppe hat Vorrang über eine Gruppe, die über das Eingabefeld *Erzwungener Benutzer* zur primären Gruppe eines Benutzers geworden ist. Wird dem Gruppennamen ein Plus-Zeichen (+) vorangestellt, wird die Gruppe nur solchen Benutzern als primäre Gruppe zugeschrieben, die bereits Mitglied dieser Gruppe sind. Alle anderen Benutzer behalten ihre gewöhnliche primäre Gruppe.
Gültige Benutzer oder Gruppen	Namen von Benutzern oder Gruppen, die auf diese Samba-Freigabe zugreifen dürfen. Alle anderen Benutzern wird der Zugriff verweigert. Wenn das Feld leer ist, dürfen alle Benutzer - gegebenenfalls mit ihrem Passwort - auf die Freigabe zugreifen. Diese Option ist nützlich, um Zugriffe auf eine Freigabe über die Dateiberechtigungen hinaus auf Ebene des Fileservers abzusichern. Die Einträge sind durch Leerzeichen zu trennen. Durch die Zeichen `@`, `+` und `&` in Verbindung mit einem Gruppennamen kann den Mitgliedern der angegebenen Gruppe die Berechtigung zum Zugriff auf die Samba-Freigabe erteilt werden: • Ein Name, der mit `@` beginnt, wird zunächst als NIS-Netgroup interpretiert. Wenn keine NIS-Netgroup mit diesem Namen gefunden wird, wird der Name als UNIX-Gruppe angesehen. • Ein Name, der mit `+` beginnt, wird ausschließlich als UNIX-Gruppe aufgefasst, ein Name, der mit `&` beginnt, ausschließlich als NIS-Netgroup. • Ein Name, der mit `+&` beginnt, wird zunächst als UNIX-Gruppe interpretiert. Wenn keine UNIX-Gruppe mit diesem Namen gefunden wird, wird der Name als NIS-Netgroup betrachtet. Die Zeichen `&+` als Namensanfang entsprechen `@`.
Nicht erlaubte Benutzer oder Gruppen	Die hier aufgeführten Benutzer oder Gruppen dürfen auf diese Samba-Freigabe nicht zugreifen. Die Syntax ist identisch zu den gültigen Benutzern. Wenn ein Benutzer oder eine Gruppe in der Liste der gültigen Benutzer und der nicht erlaubten Benutzer enthalten ist, so wird der Zugriff verweigert.
Leseberechtigung auf diese Benutzer/Gruppen beschränken	Nur die aufgeführten Benutzer oder Gruppen erhalten Leserecht auf die Freigabe.
Schreibberechtigung auf diese Benutzer/Gruppen beschränken	Nur die aufgeführten Benutzer oder Gruppen erhalten Schreibrecht auf die Freigabe.
Zugelassene Rechner/Netze	Namen von Rechnern, die auf diese Samba-Freigabe zugreifen dürfen. Allen anderen Rechnern wird der Zugriff verweigert. Neben Rechnernamen können auch IP- oder Netzwerkadressen angegeben werden, z.B. `192.0.2.0/255.255.255.0`.
Nicht zugelassene Rechner/Netze	Das Gegenteil von den zugelassenen Rechnern. Sollte ein Rechner in beiden Listen auftauchen, so wird dem Rechner der Zugriff auf die Samba-Freigabe gestattet.
Ererbte ACLs	Bei Aktivierung dieser Option erbt jede in dieser Freigabe neu erzeugte Datei die ACL (Access Control List) des Verzeichnisses, in dem sie angelegt wird.
Neue Dateien und Verzeichnisse erhalten den Besitzer des übergeordneten Verzeichnisses	Bei Aktivierung dieser Option wird jede neu erzeugte Datei dem Besitzer des übergeordneten Verzeichnis zugeordnet und nicht dem Benutzer, der die Datei erstellt hat.
Neue Dateien und Verzeichnisse erhalten	Bei Aktivierung dieser Option werden für jede Datei oder jedes Verzeichnis, die in einer Freigabe neu erzeugt werden, automatisch die UNIX-Rechte des übergeordne-

Wenn von einem Windows-Rechner aus eine neue Datei auf einem Samba-Server angelegt wird, werden die Rechte der Datei in mehreren Schritten gesetzt:

1. Zunächst werden die DOS-Rechte in Unix-Rechte übersetzt.
2. Anschließend werden die Rechte durch den *Datei-Modus* gefiltert. Nur die Unix-Rechte, die im Datei-Modus markiert sind, bleiben erhalten. Rechte, die hier nicht gesetzt sind, werden entfernt. Die Rechte müssen also als Unix-Rechte und im Datei-Modus gesetzt sein, um erhalten zu bleiben.
3. Im nächsten Schritt werden die Rechte um die unter *Erzwinge Datei-Modus* gesetzten Rechte ergänzt. Als Ergebnis hat die Datei alle Rechte, die nach Schritt 2 oder unter *Erzwinge Datei-Modus* gesetzt sind. Rechte, die unter *Erzwinge Datei-Modus* markiert sind, werden also auf jeden Fall gesetzt.

Entsprechend erhält ein neu angelegtes Verzeichnis zunächst die Rechte, die sowohl als Unix-Rechte als auch im *Verzeichnis-Modus* gesetzt sind. Danach werden die Rechte ergänzt, die unter *Erzwinge Verzeichnis-Modus* markiert sind.

Freigaben UMC Modul - Gruppe erweiterte Samba-Rechte

Tab. 12.6: Gruppe *Erweiterte Samba-Rechte*

Attribut	Beschreibung
Datei-Modus	Die Rechte, die Samba beim Anlegen einer Datei übernehmen soll, sofern sie unter Windows gesetzt sind.
Verzeichnis-Modus	Die Rechte, die Samba beim Anlegen eines Verzeichnisses übernehmen soll, sofern sie unter Windows gesetzt sind.
Erzwinge Datei-Modus	Die Rechte, die Samba beim Anlegen einer Datei auf jeden Fall setzen soll, also unabhängig davon, ob sie unter Windows gesetzt wurden oder nicht.
Erzwinge Verzeichnis-Modus	Die Rechte, die Samba beim Anlegen eines Verzeichnisses auf jeden Fall setzen soll, also unabhängig davon, ob sie unter Windows gesetzt wurden oder nicht.

Freigaben UMC Modul - Gruppe Samba-Optionen

Tab. 12.7: Gruppe *Samba-Optionen*

Attribut	Beschreibung
VFS-Objekte	Virtual File System (VFS)-Module werden in Samba verwendet, um Aktionen vor dem Zugriff auf das Dateisystem einer Freigabe auszuführen, z.B. ein Virenscanner, der jede infizierte Datei, auf die in der Freigabe zugegriffen wird, in einem Quarantänebereich ablegt oder eine serverseitige Implementierung einer Papierkorb-Löschung von Dateien.
Verstecke Dateien	Dateien und Verzeichnisse, die unter Windows nicht sichtbar sein sollen. Die Dateien oder Verzeichnisse erhalten das Datei-Attribut *hidden*. Datei- und Verzeichnisnamen müssen unter Beachtung von Groß- und Kleinschreibung angegeben werden. Die einzelnen Einträge sind durch Schrägstriche zu trennen. Da der Schrägstrich nicht als Verzeichnistrenner eingegeben werden kann, dürfen nur Namen, aber keine Pfade eingetragen werden. Alle Dateien und Verzeichnisse mit diesen Namen innerhalb der Freigabe werden dann versteckt. Die Namen dürfen Leerzeichen und die Platzhalter `*` und `?` enthalten. Zum Beispiel versteckt `/.*/test/` alle Dateien und Verzeichnisse, die mit einem *Punkt* beginnen oder *test* heißen. **Bemerkung:** Einträge in diesem Feld beeinflussen die Geschwindigkeit von Samba, da vor Anzeige von Freigabeinhalten alle Dateien und Verzeichnisse auf Übereinstimmung mit den gesetzten Filtern geprüft werden müssen.
Postexec-Skript	Ein Skript oder ein Befehl, der auf dem Server ausgeführt werden soll, wenn die Verbindung zu dieser Freigabe beendet wird.
Preexec-Skript	Ein Skript oder ein Befehl, der auf dem Server bei jeder Verbindungsaufnahme zu dieser Freigabe ausgeführt werden soll.

Freigaben UMC Modul - Gruppe Samba-Erweiterte-Einstellungen

Tab. 12.8: Gruppe *Samba-Erweiterte-Einstellungen*

Attribut	Beschreibung
Erweiterte Einstellungen für Freigaben	Neben den standardmäßig konfigurierbaren Eigenschaften einer Samba-Freigabe ermöglicht diese Einstellung beliebige weitere Samba-Einstellungen an einer Freigabe zu setzen. Eine Liste der verfügbaren Optionen kann mit dem Befehl **`man smb.conf`** abgerufen werden. Unter *Schlüssel* ist der Name der Option anzugeben und unter *Value* der zu setzende Wert. Doppelt angegebene Konfigurationsoptionen werden nicht überprüft.

Vorsicht: Das Setzen erweiterter Samba-Einstellungen ist nur in Sonderfällen nötig. Die Optionen sollten vor dem Setzen gründlich geprüft werden, da sie unter Umständen sicherheitsrelevante Auswirkungen haben können.

12.2.4 Freigaben UMC Modul - Reiter Optionen

Tab. 12.9: Reiter *Optionen*

Attribut	Beschreibung
Für Samba-Clients exportieren	Diese Option legt fest, ob die Freigabe für Samba-Clients exportiert werden soll.
Für NFS-Clients exportieren	Diese Option legt fest, ob die Freigabe für NFS-Clients exportiert werden soll.

12.3 Unterstützung von MSDFS

Das Microsoft Distributed File System (MSDFS) ist ein verteiltes Dateisystem, das es ermöglicht, Freigaben über mehrere Server und Pfade auf eine virtuelle Ordner-Hierarchie abzubilden. Dadurch kann die Last auf verschiedene Server verteilt werden.

Das Setzen der *MSDFS-Wurzel* Option an einer Freigabe (siehe *Verwaltung von Freigaben über Univention Management Console Modul* (Seite 248)) gibt an, dass es sich bei dem freigegebenen Ordner um eine Freigabe handelt, die für MSDFS genutzt werden kann. Nur innerhalb einer solchen MSDFS-Wurzel werden Verweise auf andere Freigaben angezeigt, andernfalls werden diese ausgeblendet.

Um die Funktionen eines verteilten Dateisystems nutzen zu können, muss auf dem Fileserver die Univention Configuration Registry Variable `samba/enable-msdfs` (Seite 316) auf `yes` gesetzt werden. Anschließend muss der Samba-Dienst neu gestartet werden.

Um einen Verweis mit dem Namen `zufb` von Server `sa` in der Freigabe `fa` auf die Freigabe `fb` des Servers `sb` anzulegen, muss im Ordner `fa` folgender Befehl ausgeführt werden:

```
$ ln -s msdfs:sb\\fb zufb
```

Dieser Verweis wird in jedem MSDFS fähigem Client (z.B. *Windows 2000* und *Windows XP*) als regulärer Ordner angezeigt.

Vorsicht: Auf Wurzel-Verzeichnisse sollten nur eingeschränkte Benutzergruppen Schreibzugriff haben. Andernfalls könnten Benutzer Verweise auf andere Freigaben umlenken und so Dateien abfangen oder manipulieren. Weiterhin müssen Pfade zu den Freigaben und die Verweise komplett klein geschrieben werden. Sollten Änderungen an den Verweisen vorgenommen werden, müssen beteiligte Clients neu gestartet werden.

Weitere Informationen dazu befinden sich in Jelmer R. Vernooij and Carter [15].

12.4 Konfiguration von Dateisystem-Quota

UCS erlaubt die Limitierung des Speicherplatzes, den ein Benutzer auf einer Partition verwenden kann. Diese Schwellwerte können entweder als eine Menge von Speicherplatz (z.B. 500 MB pro Benutzer) oder als maximale Anzahl von Dateien ohne feste Größenbeschränkung angegeben werden.

Unterschieden werden dabei zwei Arten von Schwellwerten:

Hard-Limit
: Das *Hard-Limit* ist die maximale Speichermenge, die ein Benutzer in Anspruch kann. Wird sie erreicht, können keine weiteren Dateien angelegt werden.

Soft-Limit
: Wird das *Soft-Limit* erreicht - das kleiner sein muss als das Hard-Limit - und liegt der Speicherplatzverbrauch weiterhin unter dem Hard-Limit, wird dem Benutzer eine Übergangsfrist von sieben Tagen eingeräumt, um unbenutzte Daten zu löschen. Nach Ablauf der sieben Tage können keine weiteren Dateien mehr angelegt oder

verändert werden. Benutzern, die über CIFS auf ein Dateisystem mit erschöpfter Quota zugreifen, wird eine Warnung angezeigt (als Schwellwert wird dabei das Soft-Limit angesetzt).

Ein konfigurierter Quota-Wert von `0` wird als unbegrenzte Quota ausgewertet.

Quotas können entweder über das UMC-Modul *Dateisystem Quota* oder über eine Richtlinie für Freigaben definiert werden, siehe *Konfiguration von Dateisystem-Quota* (Seite 256).

Dateisystem-Quota können nur auf Partitionen mit den Dateisystemen `ext4` und `xfs` angelegt werden. Bevor Dateisystem-Quota konfiguriert werden, muss der Quota-Support pro Partition aktiviert werden, siehe *Aktivierung von Dateisystem-Quota* (Seite 256).

12.4.1 Aktivierung von Dateisystem-Quota

Im UMC-Modul *Dateisystem Quota* werden alle Partitionen aufgeführt, auf denen Quota eingerichtet werden können. Es werden nur Partitionen angezeigt, die aktuell unter einem Mount-Punkt eingebunden sind.

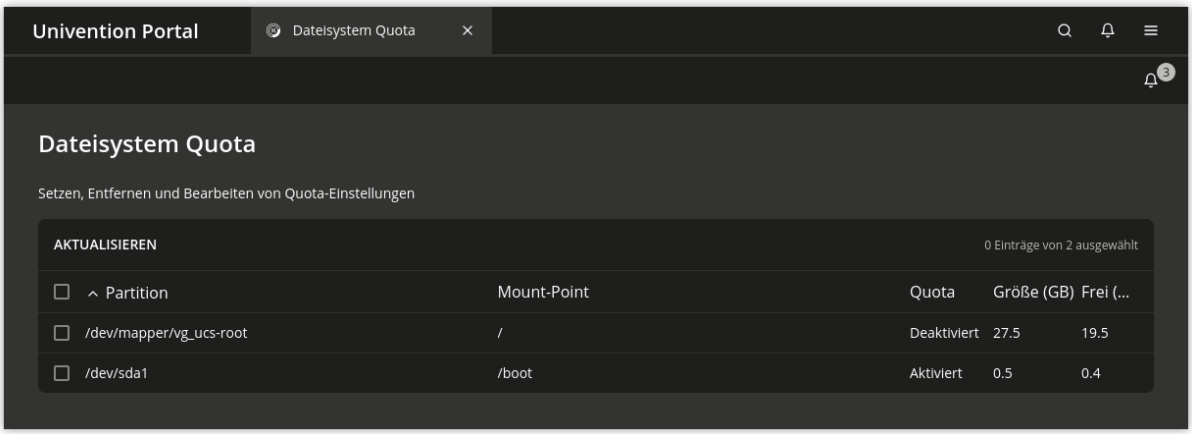


Abb. 12.2: Das UMC Modul *Dateisystem Quota*

Der aktuelle Quota-Status (Aktiviert/Deaktiviert) wird angezeigt und kann mit *Aktivieren* und *Deaktivieren* verändert werden.

Nachdem auf einer `XFS` Root-Partition Quota aktiviert wurde, muss das System neu gestartet werden.

12.4.2 Konfiguration von Dateisystem-Quota

Quotas können entweder über das UMC-Modul *Dateisystem Quota* oder über eine Richtlinie für Freigaben definiert werden, siehe *Richtlinien* (Seite 77). Die Konfiguration über die Richtlinie erlaubt die Festlegung eines Standard-Werts für alle Benutzer, während das UMC-Modul eher für die flexible Konfiguration von Benutzer-Quota für einzelne Benutzer geeignet ist.

Die benutzerspezifischen Quota können im UMC-Modul *Dateisystem Quota* editiert werden. Für alle aktivierten Partitionen können mit dem Bleistift-Symbol die erlaubten Speichermengen festgelegt werden. Alle Einstellungen werden benutzerspezifisch festgelegt. Mit *Hinzufügen* können die Schwellwerte für Soft- und Hard-Limits für einen Benutzer festgelegt werden.

Die Quota-Einstellungen können auch über eine Freigaben-Richtlinie von Typ *Benutzer-Quota* festgelegt werden. Die Einstellungen gelten für alle Benutzer einer Freigabe; es ist nicht möglich an einer Richtlinie für verschiedene Benutzer unterschiedliche Quota-Limitierungen festzulegen.

Über eine Freigabe-Richtlinie gesetzte Quotaeinstellungen werden standardmäßig nur einmal ausgewertet und auf das Dateisystem angewendet. Sollte sich die Einstellung ändern, wird dies nicht automatisch bei der nächsten Anmeldung des Benutzers angewendet. Um geänderte Quota-Werte zu übernehmen, kann an der Freigabe-Richtlinie der Punkt *Einstellungen bei jedem Login anwenden* aktiviert werden.

Quota-Richtlinien können nur auf Partitionen angewendet werden, für die die Quota-Unterstützung im UMC-Modul aktiviert wurde, siehe *Aktivierung von Dateisystem-Quota* (Seite 256).

Bemerkung: Dateisystem-Quotas können immer nur auf vollständige Partitionen angewendet werden. Auch wenn die Richtlinien für Freigaben definiert werden, werden sie auf vollständige Partitionen angewendet. Wenn also beispielsweise auf einem Server drei Freigaben bereitgestellt werden, die alle auf der separaten `/var/`-Partition abgelegt werden und werden drei verschiedene Richtlinien konfiguriert und angewendet, so gilt die restriktivste Einstellung für die komplette Partition. Wenn unterschiedliche Quota verwendet werden sollen, wird empfohlen die Daten auf individuelle Partitionen zu verteilen.

12.4.3 Auswertung von Quota bei der Anmeldung

Die im UCS-Managementsystem definierten Einstellungen werden bei der Anmeldung an UCS-Systemen durch das im PAM-Stack aufgerufene Tool **univention-user-quota** ausgewertet und aktiviert.

Wenn keine Quota eingesetzt werden soll, kann die Auswertung durch Setzen der Univention Configuration Registry Variable *quota/userdefault* (Seite 316) auf `no` deaktiviert werden.

Wird die Univention Configuration Registry Variable *quota/logfile* (Seite 316) auf einen beliebigen Dateinamen gesetzt, wird die Aktivierung der Quotas in die angegebene Datei protokolliert.

12.4.4 Abfrage des Quota-Status durch Administratoren oder Benutzer

Die für ein System definierten Quota-Begrenzungen können als Benutzer mit dem Befehl **repquota -va** aufgelistet werden, z.B.:

```
*** Report for user quotas on device /dev/vdb1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root            --      20       0       0              2     0     0
Administrator   --       0       0  102400              0     0     0
user01          --  234472 2048000 4096000              2     0     0
user02          --       0 2048000 4096000              0     0     0

Statistics:
Total blocks: 8
Data blocks: 1
Entries: 4
Used average: 4.000000
```

Angemeldete Benutzer können mit dem Befehl **quota -v** die für sie geltenden Quota-Grenzen und die aktuelle Auslastung abfragen.

Weitergehende Informationen zu den Befehlen finden sich in den Manpages der Befehle.

KAPITEL 13

Druckdienste

Univention Corporate Server beinhaltet ein Drucksystem, mit dem sich auch komplexe Umgebungen realisieren lassen. Drucker und Druckergruppen werden dabei im UMC-Modul *Drucker* verwaltet.

Die Druckdienste basieren auf *CUPS (Common Unix Printing System)*. Druckaufträge werden von CUPS in Warteschlangen verwaltet und in die Druckformate der angeschlossenen Drucker umgewandelt. Die Druckerwarteschlangen werden im UMC-Modul *Druckaufträge* verwaltet, siehe *Verwaltung von Druckaufträgen und Druckerwarteschlangen* (Seite 264).

Alle in CUPS eingerichteten Drucker können von UCS-Systemen direkt verwendet werden und werden bei Verwendung von Samba automatisch auch für Windows-Rechner bereitgestellt.

Die technischen Fähigkeiten eines Druckers werden in sogenannten PPD-Dateien spezifiziert. In diesen Dateien ist beispielsweise festgehalten, ob ein Drucker farbig drucken kann, ob ein beidseitiger Druck möglich ist, welche Papierschächte vorhanden sind, welche Auflösungen unterstützt und welche Druckerbefehlssprachen unterstützt werden (z.B. PCL oder PostScript).

Druckaufträge werden von CUPS mit Hilfe von Filtern in ein Format umgewandelt, das der jeweilige Drucker interpretieren kann, also z.B. in PostScript für einen PostScript-fähigen Drucker.

UCS bringt eine Vielzahl von Filtern und PPD-Dateien direkt mit, so dass die meisten Drucker ohne zusätzlich zu installierende Treiber angesprochen werden können. Die Einrichtung weiterer PPD-Dateien ist in *Integration weiterer PPD-Dateien* (Seite 270) beschrieben.

Ein Drucker kann entweder direkt an den Druckserver angeschlossen sein (z.B. über die USB-Schnittstelle oder einen Parallelport) oder über Remote-Protokolle mit einem Druckserver kommunizieren (z.B. TCP/IP-fähige Drucker, die über IPP oder LPD angebunden werden).

Netzwerkdrucker mit eigener IP-Adresse sollten als IP-Client im UMC-Modul *Rechner* registriert werden (siehe *UCS-Systemrollen* (Seite 35)).

CUPS bietet die Möglichkeit Druckergruppen zu definieren. Die darin enthaltenen Drucker werden abwechselnd zur Bearbeitung von Druckaufträgen herangezogen, was eine automatische Lastverteilung zwischen räumlich benachbarten Druckern ermöglicht.

Es können auch Druckerfreigaben von Windows-Systemen in den CUPS-Druckserver integriert werden, dies ist in *Konfiguration von Druckerfreigaben* (Seite 260) dokumentiert.

13.1 Installation eines Druckservers

Ein Druckserver kann mit der Applikation **Druckserver (CUPS)** aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **univention-printserver** installiert und **univention-run-join-scripts** aufgerufen werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104).

13.2 Einstellung lokaler Konfigurationseigenschaften eines Druckservers

Die Konfiguration von CUPS als Druckserver erfolgt über Einstellungen aus dem LDAP-Verzeichnisdienst und Univention Configuration Registry. Wird die Univention Configuration Registry Variable *cups/include/local* (Seite 304) auf `true` gesetzt, wird zusätzlich die Datei `/etc/cups/cupsd.local.conf` eingebunden, in der beliebige weitere Optionen hinterlegt werden können. Änderungen an dieser Datei benötigen **ucr commit /etc/cups/cupsd.conf** um aktiv zu werden.

Tritt bei der Verarbeitung einer Drucker-Warteschlange ein Fehler auf (z.B. weil der angebundene Drucker ausgeschaltet ist), wird in der Grundeinstellung die weitere Bearbeitung der Warteschlange gestoppt. Diese muss dann durch den Administrator wieder aktiviert werden (siehe *Verwaltung von Druckaufträgen und Druckerwarteschlangen* (Seite 264)). Wird die Univention Configuration Registry Variable *cups/errorpolicy* (Seite 304) auf *retry-job* gesetzt, versucht CUPS alle dreißig Sekunden automatisch erfolglose Druckaufträge erneut durchzuführen.

13.3 Konfiguration von Druckerfreigaben

Druckerfreigaben werden im UMC-Modul *Drucker* mit dem Objekttyp *Druckerfreigabe: Drucker* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)).

Beim Hinzufügen, Entfernen oder Bearbeiten einer Druckerfreigabe wird der Drucker automatisch auch in CUPS konfiguriert. CUPS verfügt über keine LDAP-Schnittstelle für die Druckerkonfiguration, stattdessen wird über ein Listener-Modul die CUPS-Druckerkonfiguration (`printers.conf`) generiert. Wenn Samba eingesetzt wird, werden die Druckerfreigaben automatisch auch für Windows-Clients bereitgestellt.

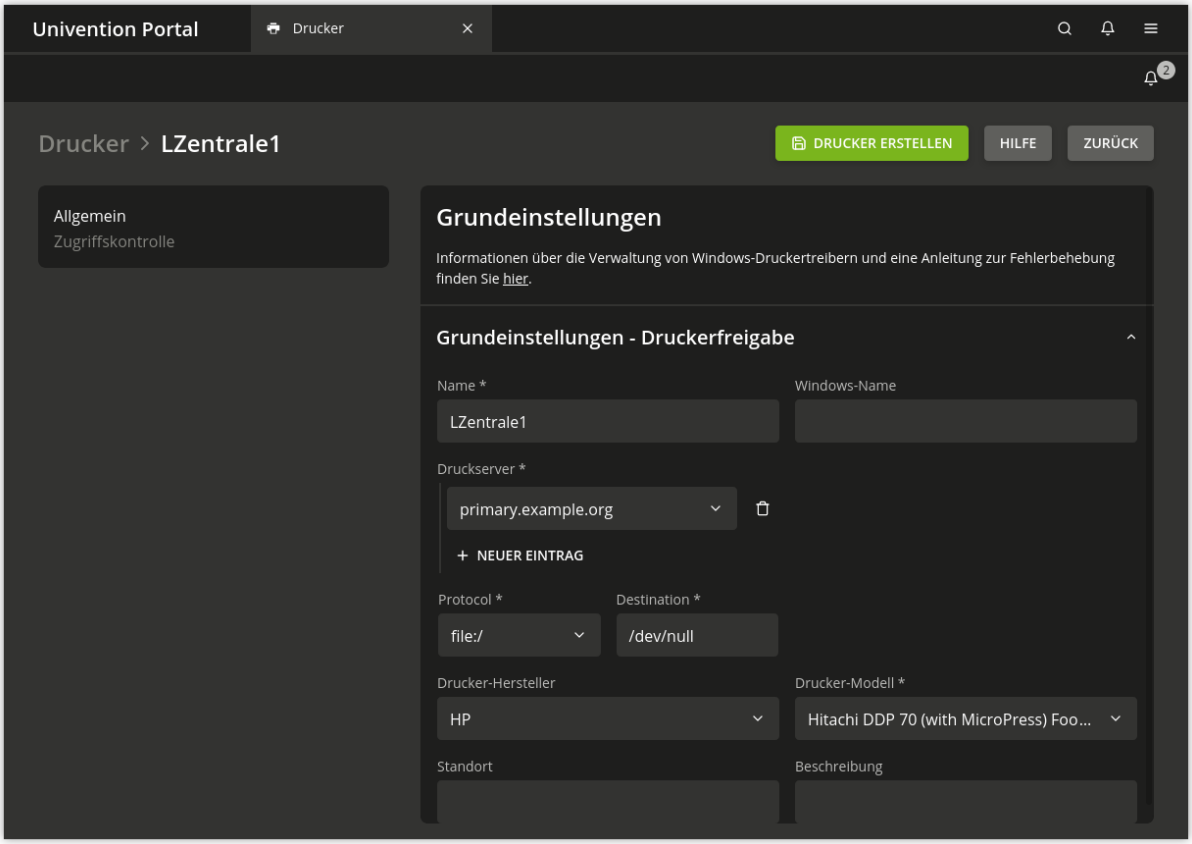


Abb. 13.1: Konfiguration von Druckerfreigaben

13.3.1 Drucker UMC Modul - Reiter Allgemein

Tab. 13.1: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Dieses Eingabefeld enthält den Namen der Druckerfreigabe, der von CUPS verwendet wird. Unter diesem Namen erscheint der Drucker unter Linux und Windows. Der Name darf alphanumerische Zeichen (also die Buchstaben `a` bis `z` in Groß- und Kleinschreibung und die Ziffern `0` bis `9`) sowie Binde- und Unterstriche enthalten. Andere Zeichen (einschließlich Leerzeichen) sind nicht erlaubt.
Druckserver (*)	Ein Druckserver verwaltet die Druckerqueue für den freizugebenden Drucker und wandelt - falls notwendig - die Druckdaten in das passende Druckerformat um. Ist der Drucker nicht bereit, speichert der Druckserver die anstehenden Druckaufträge zwischen und sendet sie später zum Drucker. Werden mehrere Druckserver angegeben, wird der Druckauftrag vom Client zum ersten Druckserver gesendet, der erreichbar ist. Nur UCS Directory Nodes und Managed Nodes, auf denen das Paket **univention-printserver** installiert wurde, werden in der Liste angezeigt.
Protokoll und Ziel (*)	Diese beiden Eingabefelder legen fest, wie der Druckserver auf den Drucker zugreift. Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die Konfiguration lokal an den Server angeschlossener Drucker: • `parallel://`*`devicefile`* Beispiel: `parallel://dev/lp0` • `socket://`*`server`*`:`*`port`* Beispiel: `socket://printer_03:9100` • `usb://`*`devicefile`* Beispiel: `usb://dev/usb/lp0` Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die Konfiguration von Netzwerk-Druckern: • `http://`*`server`*`[:`*`port`*`]/`*`path`* Beispiel: `http://192.0.2.10:631/printers/remote` • `ipp://`*`server`*`/printers/`*`queue`* Beispiel: `ipp://printer_01/printers/xerox` • `lpd://`*`server`*`/`*`queue`* Beispiel: `lpd://192.0.2.30/bwdraft` Das Protokoll `cups-pdf` wird zur Anbindung eines Pseudodruckers verwendet, der aus allen Druckaufträgen ein PDF-Dokument erzeugt. Die Einrichtung ist in *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 265) dokumentiert. Das Protokoll `file://` erwartet als Ziel einen Dateinamen. Der Druckauftrag wird dann nicht auf einen Drucker geschrieben, sondern in diese Datei, was für Testzwecke nützlich sein kann. Die Datei wird mit jedem Druckauftrag neu geschrieben. Mit dem Protokoll `smb://` kann eine Windows-Druckerfreigabe eingebunden werden. Um beispielsweise die Druckerfreigabe *laser01* des Windows-Systems *win01* einzubinden, muss als Ziel *win01/laser01* angegeben werden. Dabei sollten Hersteller und Modell-Typ entsprechend des verwendeten Geräts gewählt werden. Der Druckserver nutzt dabei die verwendeten Druckermodell-Einstellungen um die Druckaufträge gegebenenfalls umzuwandeln und sendet diese anschließend an die URI `smb://win01/laser01`. Hierbei werden keine Windows-Treiber verwendet. Unabhängig von diesen Einstellungen kann die Druckerfreigabe auch weiterhin von anderen Windows-Systemen mit den entsprechenden Druckertreibern eingebunden werden.
Drucker-Hersteller	Nach der Auswahl des Herstellers des Druckers wird die Auswahlliste *Drucker-Modell* automatisch aktualisiert.
Drucker-Modell (*)	Diese Auswahlliste zeigt alle verfügbaren Drucker-PPD-Dateien für den ausgewählten *Drucker-Hersteller* an. Wenn das gesuchte Drucker-Modell nicht vorhanden ist, kann ein ähnliches Modell ausgewählt werden und mit einem Drucktest die korrekte Funktion überprüft werden. In *Integration weiterer PPD-Dateien* (Seite 270) wird erläutert, wie die Liste der Drucker-Modelle erweitert werden kann.
Samba-Name	Für einen Drucker kann ein zusätzlicher Name vergeben werden, unter dem er von Windows aus erreichbar sein soll. Im Gegensatz zum CUPS-Namen (siehe *Name*) darf der Samba-Name Leerzeichen und Umlaute enthalten. Der Drucker steht für Windows dann sowohl unter dem CUPS-Namen als auch unter dem Samba-Namen zur Verfügung. Die Verwendung des Samba-Namens zusätzlich zum CUPS-Namen ist z.B. dann

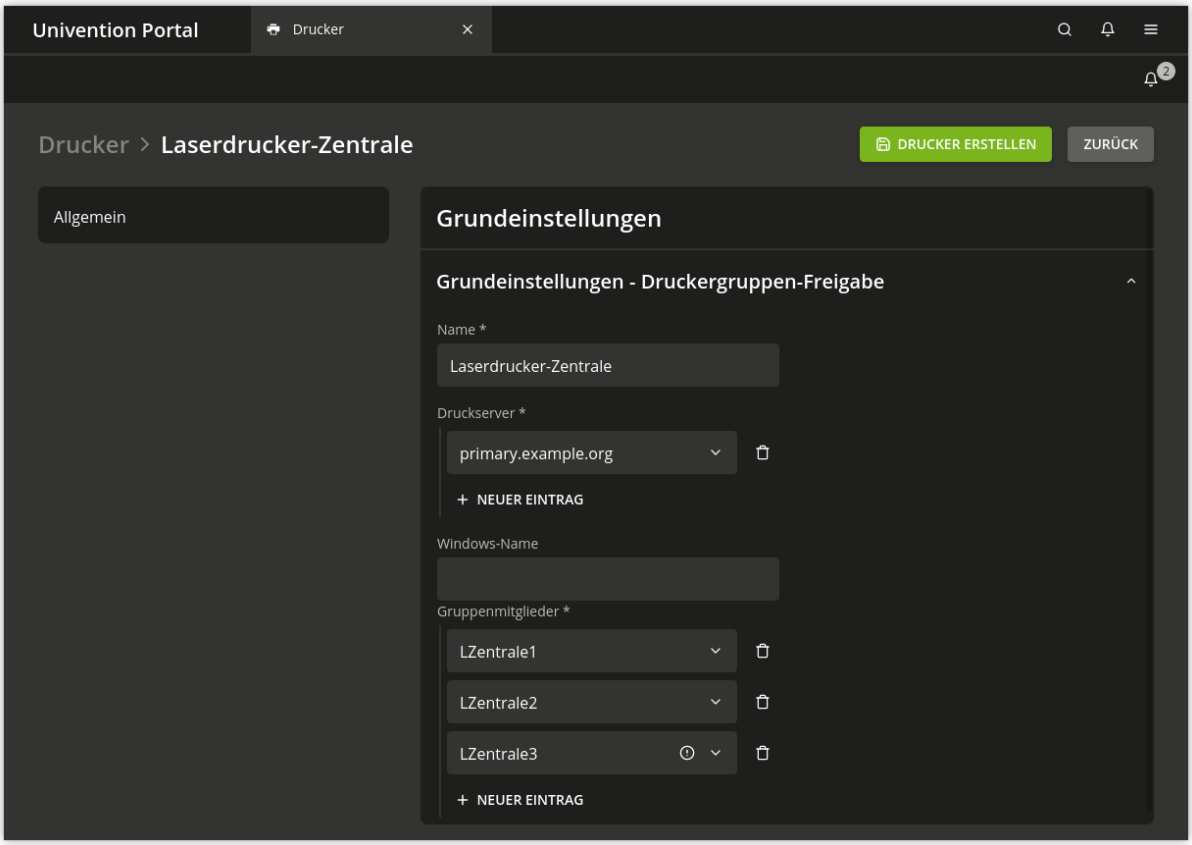
13.3.2 Drucker UMC Modul - Reiter Zugriffskontrolle

Tab. 13.2: Reiter *Zugriffskontrolle*

Attribut	Beschreibung
Zugriffskontrolle	Über diese Auswahl lassen sich Zugriffsrechte für den Drucker festlegen. Der Zugriff kann auf bestimmte Gruppen oder Benutzer beschränkt werden oder er kann generell freigegeben und spezifisch für bestimmte Gruppen oder Benutzer gesperrt werden. Standardmäßig ist der Zugriff für alle Gruppen und Benutzer zugelassen. Diese Rechte werden auch für die entsprechende Samba-Druckerfreigabe übernommen, so dass beim Drucken über Samba die gleichen Zugriffsrechte gelten, wie beim Drucken direkt über CUPS. Die Zugriffskontrolle ist z.B. sinnvoll für die Verwaltung von Druckern an mehreren Standorten, so dass den Benutzern an Standort A nicht die Druckerfreigaben von Standort B angezeigt werden.
Zugelassene/abgewiesene Benutzer	Diese Auswahl führt einzelne Benutzer auf, für die der Zugriff reguliert werden soll.
Zugelassene/abgewiesene Gruppen	Diese Auswahl führt Gruppen auf, für die der Zugriff reguliert werden soll.

13.4 Konfiguration von Druckergruppen

CUPS bietet die Möglichkeit Drucker in Klassen zusammenzufassen. In UCS sind diese als *Druckergruppen* implementiert. Druckergruppen erscheinen für Clients wie normale Drucker. Eine Druckergruppe erhöht die Verfügbarkeit des Druckdienstes. Wird auf eine Druckergruppe gedruckt, wird der Auftrag an den ersten verfügbaren Drucker der Druckergruppe geschickt. Die Auswahl der Drucker erfolgt nach dem *Round Robin Prinzip*, so dass eine gleichmäßige Auslastung angestrebt wird.



Eine Druckergruppe muss mindestens einen Drucker als Mitglied haben. Es können nur Drucker des gleichen Druckservers als Mitglieder der Gruppe gesetzt werden.

Vorsicht: Die Fähigkeit, Druckerfreigaben von verschiedenen Druckservern in einer Druckergruppe zusammenzufassen, ermöglicht es auch, Druckergruppen als Mitglieder einer Druckergruppe zu setzen. Eine Druckergruppe könnte sich dadurch selbst als Gruppenmitglied enthalten. Dies ist unbedingt zu vermeiden.

Druckergruppen werden im UMC-Modul *Drucker* mit dem Objekttyp *Druckerfreigabe: Druckergruppe* verwaltet (siehe auch *Univention Management Console-Module* (Seite 72)).

Tab. 13.3: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Dieses Eingabefeld enthält den Namen der Druckergruppenfreigabe, der von CUPS verwendet wird. Unter diesem Namen erscheint die Druckergruppe unter Linux und Windows. Der Name darf alphanumerische Zeichen (also die Buchstaben `a` bis `z` in Groß- und Kleinschreibung und die Ziffern `0` bis `9`) sowie Binde- und Unterstriche enthalten. Andere Zeichen (einschließlich Leerzeichen) sind nicht erlaubt.
Druckserver (*)	Drucker, die hier angegebenen Servern zugeordnet sind, können in der darunter angeordneten Auswahl in die Liste der *Gruppenmitglieder* aufgenommen werden.
Samba-Name	Für eine Druckergruppe kann ein zusätzlicher Name vergeben werden, unter dem sie von Windows aus erreichbar sein soll. Im Gegensatz zum CUPS-Namen (siehe *Name*) darf der Samba-Name Leerzeichen und Umlaute enthalten. Der Drucker steht für Windows dann sowohl unter dem CUPS-Namen als auch unter dem Samba-Namen zur Verfügung. Die Verwendung des Samba-Namens zusätzlich zum CUPS-Namen ist z.B. dann sinnvoll, wenn die Druckergruppe schon früher unter Windows mit einem Namen verwendet wurde, der Leerzeichen oder Umlaute enthielt. Die Druckergruppe kann dann weiterhin unter diesem Namen erreicht werden und die Windows-Rechner müssen nicht umkonfiguriert werden.
Gruppenmitglieder	Durch diese Liste werden Drucker der Druckergruppe zugeordnet.

13.5 Verwaltung von Druckaufträgen und Druckerwarteschlangen

Das UMC-Modul *Druckaufträge* erlaubt auf Druckservern den Status der angeschlossenen Drucker zu prüfen, angehaltene Drucker neu zu starten oder Druckaufträge aus den Warteschlagen zu entfernen.

Auf der Startseite des Moduls befindet sich eine Suchmaske, mit der die vorhandenen Drucker ausgewählt werden können. In der Ergebnisliste wird zu dem jeweiligen Drucker der Server, der Name, der Status, der Standort und die Beschreibung angezeigt. Durch Markieren der Drucker und Ausführen einer der beiden Aktionen *deaktivieren* oder *aktivieren*, kann der Status mehrerer Drucker gleichzeitig geändert werden.

Durch den Klick auf einen Druckernamen können Details zu dem ausgewählten Drucker angezeigt werden. Zu den angezeigten Informationen gehört auch eine Liste der aktuell existierenden Druckaufträge, die noch in der Warteschlange des Druckers sind. Durch Markieren der Druckaufträge und Auswahl der Aktion *Löschen* können Druckaufträge aus der Warteschlange entfernt werden.

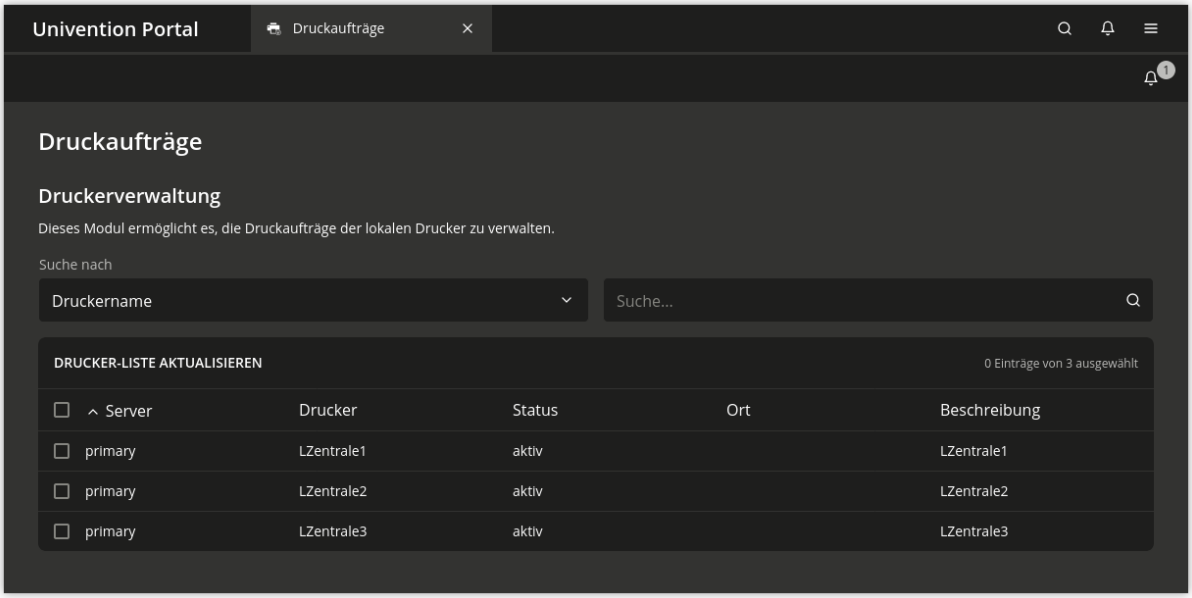


Abb. 13.2: Drucker-Administration

13.6 Generierung von PDF-Dokumenten aus Druckaufträgen

Durch die Installation des Pakets **univention-printserver-pdf** wird ein Druckserver um den speziellen Druckertyp *cups-pdf* erweitert, der eingehende Druckaufträge in das PDF-Format umwandelt und für den jeweiligen Benutzer lesbar in ein Verzeichnis auf dem Druckserver ausgibt. Nach der Installation des Pakets sollte **univention-run-join-scripts** aufgerufen werden.

Beim Anlegen eines PDF-Druckers im UMC-Modul *Drucker* (siehe *Konfiguration von Druckerfreigaben* (Seite 260)) muss als Protokoll `cups-pdf:/` ausgewählt werden, das Ziel-Feld bleibt leer.

Als *Drucker-Hersteller* muss `PDF` und als *Drucker-Modell* `Generic CUPS-PDF Printer` ausgewählt werden.

Das Zielverzeichnis für die generierten PDF-Dokumente wird über die Univention Configuration Registry Variable *cups/cups-pdf/directory* (Seite 304) festgelegt. Standardmäßig wird es auf `/var/spool/cups-pdf/%U` gesetzt, so dass **cups-pdf** für jeden Benutzer ein eigenes Verzeichnis verwendet.

Anonym eingegangene Druckaufträge werden in das durch die Univention Configuration Registry Variable *cups/cups-pdf/anonymous* (Seite 304) vorgegebene Verzeichnis ausgegeben (Standardeinstellung: `/var/spool/cups-pdf/`).

In der Grundeinstellung werden die generierten PDF-Dokumente unbegrenzt aufbewahrt. Wird die Univention Configuration Registry Variable *cups/cups-pdf/cleanup/enabled* (Seite 304) auf `true` gesetzt werden alte PDF-Druckaufträge über einen Cron-Job gelöscht. Die Aufbewahrungszeit in Tagen kann mit der Univention Configuration Registry Variable *cups/cups-pdf/cleanup/keep* (Seite 304) konfiguriert werden.

13.7 Einbinden von Druckerfreigaben auf Windows-Clients

Die im UMC-Modul *Drucker* eingerichteten Druckerfreigaben können auf Windows-Systemen als Netzwerkdrucker hinzugefügt werden. Dies erfolgt über die Systemsteuerung unter *Drucker ▸ Netzwerkdrucker hinzufügen*. Die Druckertreiber müssen beim ersten Zugriff eingerichtet werden. Wurden die Treiber serverseitig hinterlegt (siehe unten), erfolgt die Zuweisung des Treibers automatisch.

Druckerfreigaben werden in der Regel mit den mitgelieferten Windows-Druckertreibern betrieben. Der Netzwerkdrucker kann auf Windows-Seite alternativ mit einem Standard-PostScript-Druckertreiber eingerichtet werden. Wenn auf einen Farbdrucker zugegriffen werden soll, sollte auf Windows-Seite ein Treiber für einen PostScript-fähigen Farbdrucker verwendet werden, z.B. *HP Color LaserJet 8550*.

Vorsicht: Der Zugriff auf einen Drucker ist für einen regulären Benutzer nur möglich, wenn dieser über lokale Rechte zur Treiberinstallation verfügt oder ein entsprechender Druckertreiber auf dem Druckserver hinterlegt wurde. Ist dies nicht der Fall kann es zu einer Windows Fehlermeldung kommen, die besagt, dass die Berechtigungen nicht ausreichen, um eine Verbindung mit dem Drucker herzustellen.

Windows unterstützt ein Verfahren zur serverseitigen Bereitstellung von Druckertreibern auf dem Druckserver (*Point ‚n' Print*). Die folgende Anleitung beschreibt die Bereitstellung der Druckertreiber unter Windows für eine im UMC-Modul *Drucker* konfigurierte Druckerfreigabe. Zuerst müssen die Druckertreiber auf dem Druckserver hinterlegt werden, danach werden die Drucker mit einem Druckertreiber verknüpft. Die Benutzerführung unter Windows bietet zahlreiche Stolperfallen, es ist wichtig den einzelnen Schritten exakt zu folgen.

1. Zuerst müssen die Druckertreiber von der Webseite des Herstellers heruntergeladen werden. Wird eine Umgebung verwendet, in der die 64 Bit-Versionen von Windows eingesetzt werden, müssen die Treiber unbedingt in beiden Versionen bezogen werden (32 und 64 Bit). Benötigt werden die `INF`-Dateien.

2. Nun muss das Programm **`printmanagement.msc`** (Druckerverwaltung) gestartet werden. Im Menüpunkt *Aktion* kann mit einem Klick auf *Server hinzufügen/entfernen* ein weiterer Server hinzugefügt werden. In dem Eingabefeld *Server hinzufügen* muss der Name des Druckerservers eingetragen werden.

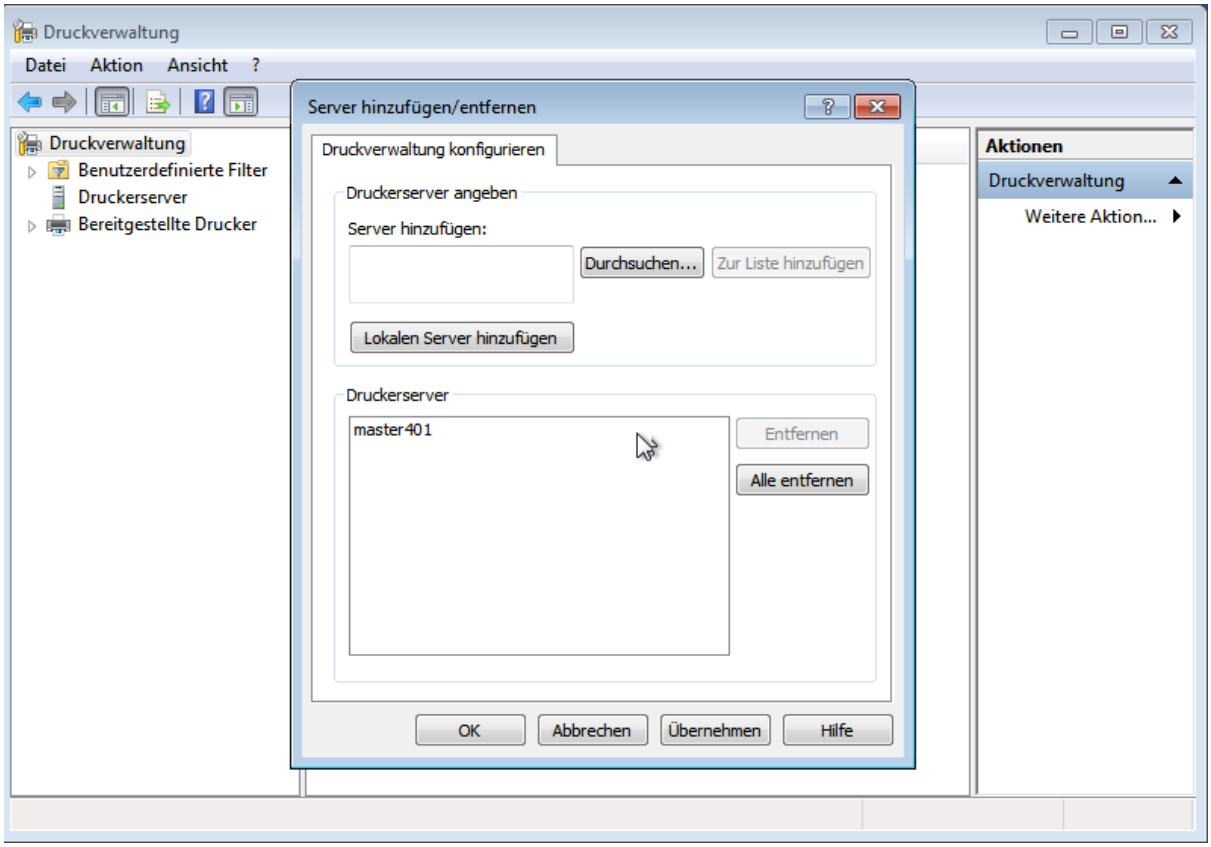


Abb. 13.3: Druckerserver hinzufügen

3. In der Druckerverwaltung sollte der neu hinzugefügte Druckserver nun aufgelistet werden. Durch einen Klick auf *Drucker* werden die aktuell auf dem Druckerserver eingerichteten Druckerfreigaben angezeigt.

4. Mit einem Klick auf den Eintrag *Treiber* werden die hinterlegten Druckertreiber aufgelistet. Im Menüpunkt *Aktion* kann mit einem Klick auf *Treiber hinzufügen* der Dialog für die Treiberinstallation gestartet werden.

   Wir empfehlen die Druckertreiber direkt vom Hersteller herunterzuladen und diese während der Treiberinstallation auszuwählen. Wird eine Umgebung verwendet, in der die 64 Bit-Versionen von Windows eingesetzt werden, sollte zunächst geprüft werden, ob auf dem UCS Samba System die Univention Configuration Registry Variable *samba/spoolss/architecture* (Seite 316) auf `Windows x64` gesetzt ist. Falls das nicht der Fall ist, müssen die Treiber unbedingt für 32 und 64 Bit hochgeladen werden, andernfalls kann auf

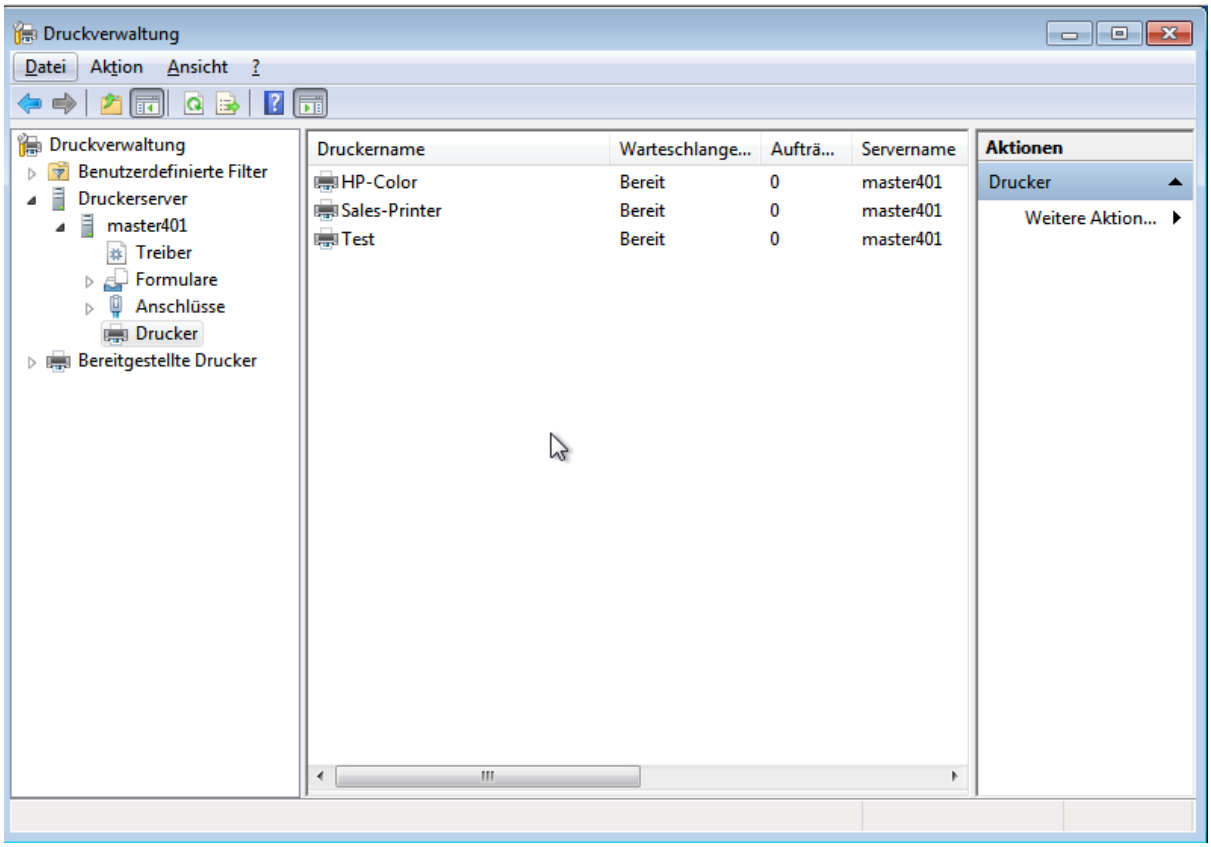


Abb. 13.4: Druckerliste

die 32 Bit Treiber verzichtet werden, wenn ausschliesslich 64 Bit Windows Systeme in der Domäne zum Einsatz kommen. Die Treiber können für verschiedene Windows-Architekturen entweder in getrennten Schritten nacheinander oder direkt in einem Vorgang hochgeladen werden.

Falls beide Treiberarchitekturen gleichzeitig zum Hochladen ausgewählt werden, dann muss im anschließenden Dateiauswahldialog als erstes der 64 Bit Treiber gewählt werden. Nachdem Windows diese Dateien zum Server hochgeladen hat, fragt es dann erneut nach dem Ort für die 32 Bit Treiber. Danach werden auch diese zum Server hochgeladen.

5. Nach diesen Schritten sind die Treiber auf dem UCS Druckserver im Verzeichnis `/var/lib/samba/drivers/` gespeichert.

6. Nun muss die Druckerfreigabe noch mit dem hochgeladenen Druckertreiber verknüpft werden. Dazu wird im Programm **`printmanagement.msc`** die Liste der vom Druckserver bereitgestellten Drucker aufgerufen. Dort werden durch einen Doppelklick auf den *Drucker* die Eigenschaften aufgelistet.

7. Ist noch kein Druckertreiber hinterlegt, wird eine Meldung angezeigt, dass noch kein Druckertreiber installiert ist. Die Frage, ob der Treiber installiert werden soll, muss hier mit *Nein* bestätigt werden.

8. Nun muss im Reiter *Erweitert* unter *Treiber* der hochgeladene Treiber aus dem Dropdown-Menü ausgewählt werden. Anschließend muss auf *Übernehmen* geklickt werden (Wichtig: **NICHT** auf *OK*!).

9. Falls der betreffende Druckertreiber das erste mal einem Drucker zugewiesen wird, dann wird ein Dialog angezeigt, in dem gefragt wird, ob dem Drucker vertraut wird. Dies muss mit *Treiber installieren* bestätigt werden. Nun werden die serverseitig hinterlegten Druckertreiber auf den Client heruntergeladen. Falls der betreffende Druckertreiber schon zuvor einmal auf diese Weise vom Druckerserver auf das betreffende Windows System heruntergeladen worden ist, dann meldet Windows an dieser Stelle eine Fehlermeldung `0x0000007a`. Diese kann ignoriert werden.

10. **Wichtig**: Nun sollte nicht direkt auf *OK* geklickt werden, sondern es muss noch einmal auf den Reiter *Allgemein* gewechselt werden. Auf dem Reiter muss weiterhin der alte Name der Druckerfreigabe angezeigt werden.

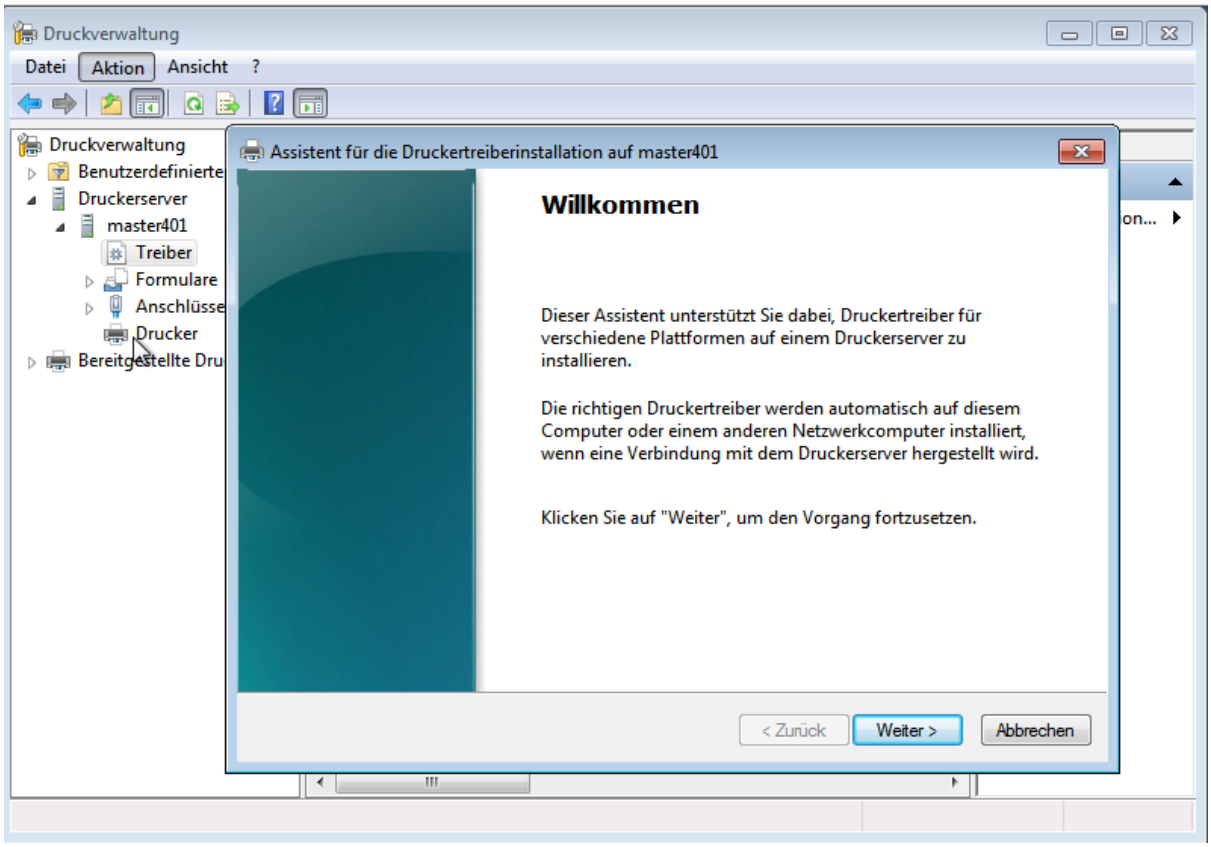


Abb. 13.5: Treiberinstallation

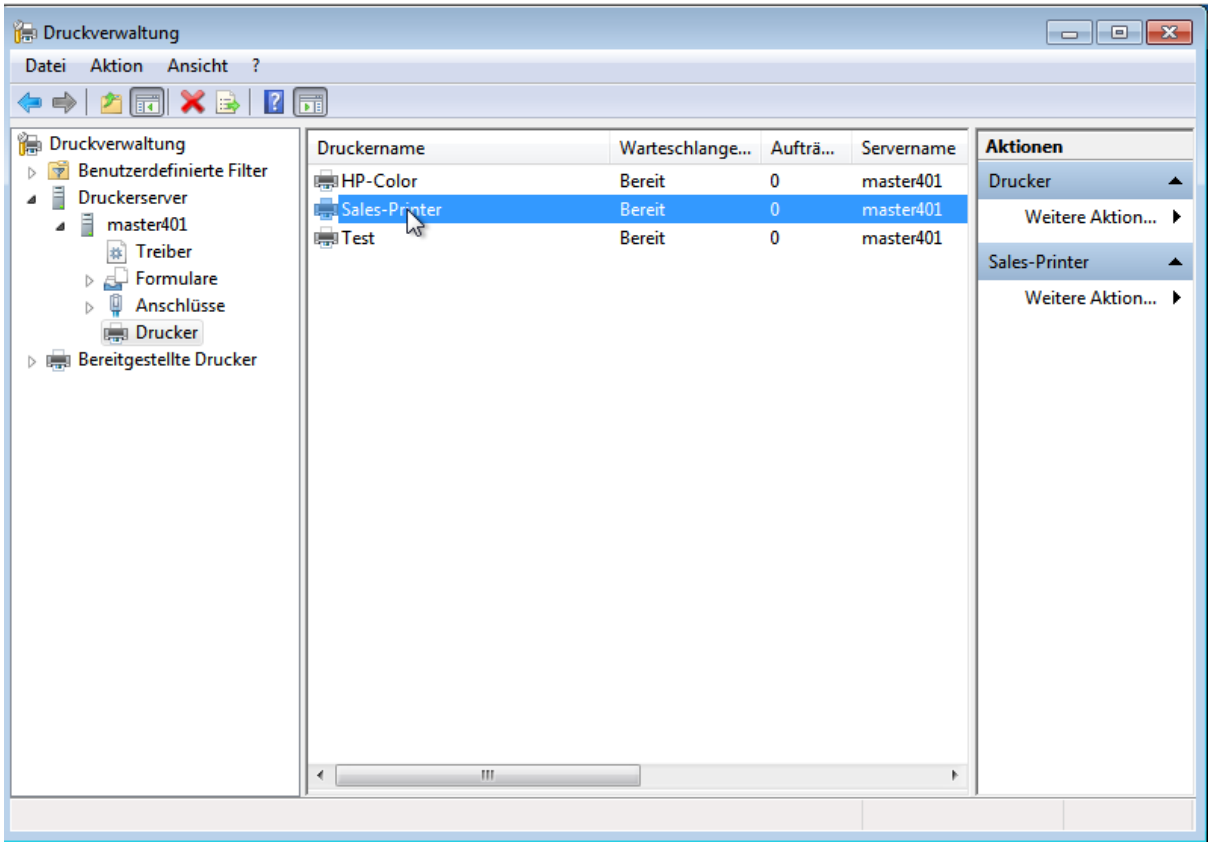


Abb. 13.6: Drucker auswählen

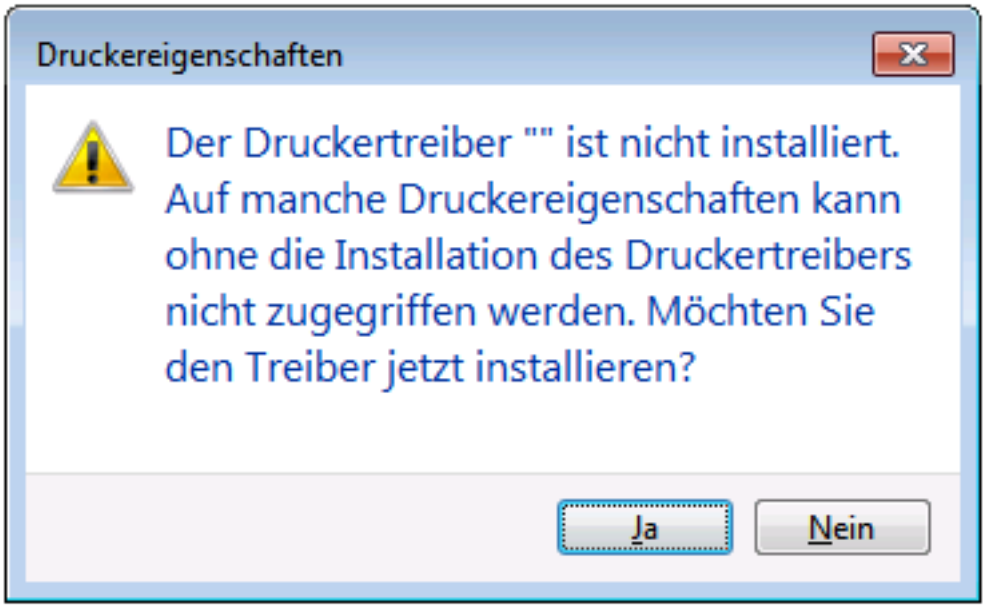


Abb. 13.7: Fehlermeldung beim ersten Zugriff

In UCS Releases vor UCS 4.0-1 kann es vorkommen, dass das Windows System hier den Namen der Druckerfreigabe in den Namen des Druckertreibers geändert hat. Wenn man dies so übernehmen würde, dann wäre der Drucker nicht mehr mit der Freigabe assoziiert!

Wenn dieser Fall eingetreten ist, muss der Name des Druckers auf dem Reiter *Allgemein* (das erste Eingabefeld, neben dem stilisierten Druckersymbol) wieder auf den Namen der Druckerfreigabe geändert werden. Hier ist das im UMC-Modul *Drucker* konfigurierte Feld *Windows-Name* zu verwenden (oder falls dies leer gelassen wurde, dann der Wert aus *Name*). Wenn der Name auf diese Weise zurückgesetzt werden musste, dann fragt Windows beim abschließenden Klick auf *OK* nach, ob man sich sicher ist, dass man den Namen ändern möchte. Dies ist zu bestätigen.

11. Um dem Windows Druckertreiber nun die Möglichkeit zu geben, korrekte Standard-Einstellungen für den Drucker zu speichern, sollte nun auf den Reiter *Geräteeinstellungen* gewechselt werden. Der Name dieses Reiters ist herstellerspezifisch und kann auch mit *Einstellungen* oder einfach *Konfiguration* bezeichnet sein.

    Ein abschließender Klick auf *OK* schließt den Dialog. Danach kann direkt eine Testseite gedruckt werden. Sollte Windows hier eine Fehlermeldung `0x00000006` ausgeben, muss in den Druckereinstellungen erneut geprüft werden, ob sich ein herstellerspezifischer Reiter namens *Geräteeinstellungen* (oder ähnlich) findet. Dieser sollte geöffnet und dann einfach mit *OK* bestätigt werden. Dies schließt den Dialog und speichert Druckertreibereinstellungen (`PrinterDriverData`) in der Samba Registry.

12. Es ist sinnvoll zu diesem Zeitpunkt auch direkt die Papiergröße und ähnliche Einstellungen vorzunehmen, damit diese an der Druckerfreigabe gespeichert werden. Andere Windows Systeme, die später auf die Druckerfreigabe zugreifen, finden dann automatisch die korrekten Einstellungen. Diese Einstellungen lassen sich in den meisten Fällen dadurch öffnen, indem in den Druckereigenschaften auf dem Reiter *Erweitert* auf die Schaltfläche *Standardwerte…* geklickt wird. Der sich öffnende Dialog ist ebenfalls herstellerabhängig. Typischerweise findet sich die Einstellung für Papiergröße und Orientierung auf einem Reiter *Seite Einrichten* oder auch *Papier/Qualität*. Nach Bestätigung des Dialogs durch Klick auf *OK* speichert der Druckertreiber diese Einstellungen (als `Default DevMode`) für den Drucker in der Samba Registry.

13.8 Integration weiterer PPD-Dateien

Die technischen Fähigkeiten eines Druckers werden in sogenannten PPD-Dateien spezifiziert. In diesen Dateien ist beispielsweise festgehalten, ob ein Drucker farbig drucken kann, ob ein beidseitiger Druck möglich ist, welche Papierschächte vorhanden sind, welche Auflösungen unterstützt und welche Druckerbefehlssprachen unterstützt werden (z.B. PCL oder PostScript).

Neben den bereits im Standardumfang enthaltenen PPD-Dateien können weitere über UMC-Module hinzugefügt werden. Die PPD wird in der Regel vom Hersteller des Druckers bereitgestellt und muss auf den Druckservern in das Verzeichnis `/usr/share/ppd/` kopiert werden.

Die Druckertreiberlisten werden im UMC-Modul *LDAP-Verzeichnis* verwaltet. Dort muss in den Container `univention` und dort in den Untercontainer `cups` gewechselt werden. Für die meisten Druckerhersteller existieren bereits Druckertreiberlisten. Diese können ergänzt werden oder eine neue hinzugefügt werden.

Tab. 13.4: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Der Name der Druckertreiberliste. Unter diesem Namen erscheint die Liste in der Auswahlliste *Drucker-Hersteller* auf der Karteikarte *Allgemein* der Druckerfreigaben (siehe *Konfiguration von Druckerfreigaben* (Seite 260)).
Treiber	Der Pfad zur PPD-Datei, relativ zu dem Verzeichnis `/usr/share/ppd/`. Soll beispielweise die Datei `/usr/share/ppd/laserjet.ppd` verwendet werden, so ist hier `laserjet.ppd` einzutragen. Es können auch **`gzip`**-komprimierte Dateien (Dateiendung `.gz`) angegeben werden.
Beschreibung	Eine Beschreibung des Druckertreibers, unter der er in der Auswahlliste *Drucker-Modell* auf der Reiter *Allgemein* der Druckerfreigaben erscheint.

KAPITEL 14

Maildienste

Univention Corporate Server (UCS) stellt Maildienste bereit, auf die Benutzer über Standard-Mail-Clients wie Thunderbird zugreifen können.

Für den Mailempfang und -versand wird **Postfix** verwendet. In der Grundinstallation wird auf jedem UCS-System eine für die lokale Mailzustellung ausgelegte Konfiguration eingerichtet. Postfix nimmt in dieser Konfiguration E-Mails nur vom lokalen System entgegen, und auch die Zustellung erfolgt nur für lokale Systembenutzer.

Durch die Installation der Mailserver-Komponente wird ein vollständiger Mailtransport über SMTP umgesetzt (siehe *Installation* (Seite 272)). Postfix wird bei der Installation der Komponente umkonfiguriert, so dass bei eingehenden E-Mails eine Gültigkeitsüberprüfung in Form einer Suche im LDAP-Verzeichnis durchgeführt wird. Das bedeutet, dass E-Mails nur für im LDAP-Verzeichnis eingetragene oder über einen Alias definierte E-Mail-Adressen akzeptiert werden.

Mit der Mailserver-Komponente wird ebenfalls der IMAP-Dienst **Dovecot** auf dem System installiert. Dieser stellt E-Mailkonten für die Benutzer der Domäne bereit und bietet entsprechende Schnittstellen für den Zugriff durch E-Mail-Clients an. Dovecot ist für den Abruf von E-Mails über IMAP und POP3 vorkonfiguriert. Der Zugriff über POP3 kann durch Setzen der Univention Configuration Registry Variable *mail/dovecot/pop3* (Seite 311) auf `no` deaktiviert werden. Das gleiche gilt für IMAP und die Univention Configuration Registry Variable *mail/dovecot/imap* (Seite 311). Auch die weitere Konfiguration der Mailserver erfolgt über Univention Configuration Registry (siehe *Konfiguration des Mailservers* (Seite 280)).

Die Verwaltung der Benutzerdaten des Mailservers (z.B. E-Mail-Adressen oder Verteiler) erfolgt über UMC-Module und ist in *Verwaltung der Mailserver-Daten* (Seite 272) dokumentiert. Benutzerdaten werden in LDAP gespeichert. Die Authentifizierung wird anhand der primären E-Mail-Adresse eines Benutzers durchgeführt, d.h. sie muss als Benutzername in Mail-Clients eingetragen werden. Sobald einem Benutzer im LDAP-Verzeichnis eine primäre E-Mail-Adresse zugeordnet wird, legt ein Listener-Modul ein IMAP-Postfach auf dem Mail Home Server an. Durch die Angabe eines Mail Home Servers können E-Mail-Konten der Benutzer auch auf mehrere Mailserver verteilt werden (siehe *Verteilung einer Installation auf mehrere Mailserver* (Seite 284)).

Optional können durch Postfix empfangene E-Mails vor der weiteren Verarbeitung durch Dovecot auf Spam-Inhalte und Viren hin untersucht werden. Spam-Mails werden über die Klassifizierungssoftware **SpamAssassin** erkannt (*Spamerkennung und -filterung* (Seite 277)), für die Erkennung von Viren und anderer Malware wird **ClamAV** eingesetzt (*Viren- und Malwareerkennung* (Seite 278)).

In der Voreinstellung werden E-Mails an fremde Domänen direkt dem zuständigen SMTP-Server der Domäne zugestellt. Die Ermittlung erfolgt dabei durch die Auflösung des MX-Records im DNS. Der Mailversand kann auch von einem Relay-Host z.B. beim Internet-Provider übernommen werden (siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 280)).

Das UCS-Mailsystem bietet keine Groupware-Funktionalität wie gemeinsam genutzte Kalender oder Termineinladungen. Es existieren aber auf UCS basierende Groupwaresysteme, die sich in das UCS-Managementsystem integrieren, z.B. Kopano oder Open-Xchange. Weiterführende Informationen finden sich im Univention App Center (siehe *Univention App Center* (Seite 96)).

14.1 Installation

Ein Mailserver kann mit der Applikation *Mailserver* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket **univention-mail-server** installiert werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 104). Mailserver können auf allen Server-Systemrollen installiert werden. Die Verwendung eines UCS Directory Nodes wird wegen häufiger LDAP-Zugriffe empfohlen.

Die Laufzeitdaten des Dovecot-Servers werden im Verzeichnis `/var/spool/dovecot/` abgelegt. Falls dieses Verzeichnis auf einem NFS-Laufwerk liegen sollte, lesen Sie bitte *Mailserver-Speicher auf NFS* (Seite 285).

14.2 Verwaltung der Mailserver-Daten

14.2.1 Verwaltung von Mail-Domänen

Eine Mail-Domäne ist ein gemeinsamer Namensraum für E-Mail-Adressen, Mailinglisten und IMAP-Gruppen-Ordner. Postfix unterscheidet bei der Zustellung von E-Mails zwischen lokalen und externen Domänen. Nur für E-Mail-Adressen lokaler Domänen wird die Mailzustellung vorgenommen. Der Name einer Mail-Domäne darf nur aus Kleinbuchstaben, den Ziffern 0-9, Punkten und Bindestrichen bestehen.

Mit UCS lassen sich mehrere Mail-Domänen verwalten. Die verwalteten Mail-Domänen müssen dabei nicht der DNS-Domäne des Servers entsprechen, sondern sind frei wählbar. Die auf einem Mailserver registrierten Mail-Domänen werden automatisch in der Univention Configuration Registry Variable `mail/hosteddomains` (Seite 312) gespeichert.

Damit auch externe Absender E-Mails an die Mitglieder der Domäne versenden können, müssen in der Konfiguration der autoritativen DNS-Nameserver MX-Records angelegt werden, die den UCS-Server als Mailserver für die Domäne ausweisen. Diese DNS-Anpassungen werden üblicherweise von Internet-Providern vorgenommen.

Mail-Domänen werden im UMC-Modul *E-Mail* mit dem Objekttyp *Mail-Domäne* verwaltet.

14.2.2 Zuordnung von E-Mail-Adressen zu Benutzern

Einem Benutzer können drei verschiedene Arten von E-Mail-Adressen zugeordnet werden:

Primäre E-Mail-Adresse
: Die *primäre E-Mail-Adresse* wird zur Authentifizierung an Postfix und Dovecot verwendet. Primäre E-Mail-Adressen müssen eindeutig sein. Pro Benutzer kann nur eine primäre E-Mail-Adresse konfiguriert werden. Sie definiert auch das IMAP-Postfach des Benutzers. Wenn dem Benutzer ein Mail Home Server zugeordnet ist (siehe *Verteilung einer Installation auf mehrere Mailserver* (Seite 284)), wird das IMAP-Postfach automatisch durch ein Univention Directory Listener-Modul erstellt. Der Domänenanteil der E-Mail-Adresse muss im UMC-Modul *E-Mail* registriert sein (siehe *Verwaltung von Mail-Domänen* (Seite 272)).

Alternative E-Mail-Adressen
: E-Mails an *alternative E-Mail-Adressen* werden ebenfalls in das Postfach des Benutzers zugestellt. Es können beliebig viele Adressen angegeben werden. Die alternativen E-Mail-Adressen müssen nicht eindeutig sein; besitzen zwei Benutzer die gleiche Adresse, erhalten beide Benutzer alle E-Mails, die an diese Adresse gesandt werden. Der Domänenanteil der E-Mail-Adresse muss im UMC-Modul *E-Mail* registriert sein (siehe *Verwaltung von Mail-Domänen* (Seite 272)). Um E-Mails an alternative E-Mail-Adressen zu erhalten, muss ein Benutzer eine primäre E-Mail-Adresse besitzen.

Bemerkung: Wenn die Univention Configuration Registry Variable `directory/manager/mail-address/uniqueness` auf `true` gesetzt wird, müssen die *Alternativen E-Mail-Adressen* in der gesamten Domäne eindeutig sein. Keinem anderen Benutzer kann die gleiche alternative Adresse zugewiesen werden.

E-Mailadressen zur Weiterleitung

Wenn *Weiterleitungs-E-Mail-Adressen* für einen Benutzer konfiguriert sind, werden E-Mails, die er über die primäre oder über alternative E-Mail-Adressen empfängt, an diese weiter geleitet. Optional kann eine Kopie der eingehenden Nachrichten in das Postfach des Benutzers zugestellt werden. Es können beliebig viele Adressen angegeben werden. E-Mailadressen zur Weiterleitung müssen weder eindeutig, noch muss ihr Domänenanteil im UMC-Modul registriert sein.

Bemerkung: E-Mail-Adressen können die Zeichen `a-z`, die Ziffern `0-9`, Punkte (`.`), Bindestriche (`-`) und Unterstriche (_) enthalten. Als weitere Vorgabe müssen die E-Mail-Adressen mit einem Buchstaben beginnen und ein `@`-Zeichen enthalten. Um E-Mail-Adressen vergeben zu können, muss vorher mindestens eine Mail-Domäne registriert werden (siehe *Verwaltung von Mail-Domänen* (Seite 272)).

E-Mail-Adressen werden im UMC-Modul *Benutzer* verwaltet. Die *primäre E-Mail-Adresse* wird im Reiter *Allgemein* im Untermenü *Benutzer-Konto* eingetragen. *Alternative E-Mail-Adressen* können unter *Erweiterte Einstellungen* ▸ *Mail* eingetragen werden.

Bemerkung: Sobald das Benutzerkonto konfiguriert ist, kann eine Anmeldung am UCS-Mail-Stack (`IMAP`/`POP3`/`SMTP`) erfolgen. Wurde das Benutzerkonto deaktiviert (oder das Passwort geändert), ist eine Anmeldung am Mail-Stack für eine Dauer von 5 Minuten weiterhin möglich. Der Grund hierfür ist der Authentifizierungscache des Mail-Stacks. Um den Cache zu invalidieren, führen Sie

```
$ doveadm auth cache flush
```

auf dem Mailserver aus. Die Ablaufzeit des Caches kann auf dem Mailserver mit der Univention Configuration Registry Variable *mail/dovecot/auth/cache_ttl* (Seite 310) sowie *mail/dovecot/auth/cache_negative_ttl* (Seite 310) konfiguriert werden.

14.2.3 Verwaltung von Mailinglisten

Mailinglisten werden zum Austausch von E-Mails in geschlossenen Gruppen verwendet. Jede Mailingliste verfügt über eine eigene E-Mail-Adresse. Wird an diese Adresse eine E-Mail gesendet, empfangen sie alle Mitglieder der Mailingliste.

Mail-Domänen werden im UMC-Modul *E-Mail* mit dem Objekttyp *Mailingliste* verwaltet. Unter *Name* ist ein frei wählbarer Name der Mailingliste anzugeben, die Angabe einer *Beschreibung* ist optional. Als *Mail-Adresse* ist die E-Mail-Adresse der Mailingliste einzugeben. Der Domänenteil der Adresse muss dabei einer der verwalteten Mail-Domänen entsprechen. Unter *Mitglieder* können beliebig viele Adressen aufgenommen werden, im Gegensatz zu Mailgruppen (siehe *Verwaltung von Mailgruppen* (Seite 274)) können hier auch externe E-Mail-Adressen aufgenommen werden. Nach dem Anlegen einer Mailingliste ist diese umgehend verfügbar.

In der Grundeinstellung kann jeder an die Mailingliste schreiben. Um Missbrauch zu verhindern, besteht die Möglichkeit den Senderkreis einzuschränken. Dazu muss die Univention Configuration Registry Variable *mail/postfix/policy/listfilter* (Seite 312) auf dem Mailserver auf `yes` gesetzt und Postfix neu gestartet werden. Unter *Erweiterte Einstellungen* können dann *Benutzer, die berechtigt sind, E-Mails an diese Liste zu versenden* und *Gruppen, die berechtigt sind, E-Mails an diese Liste zu versenden* festgelegt werden. Ist hier ein Feld gesetzt, ist das Senden nur den berechtigten Nutzern/Gruppen erlaubt.

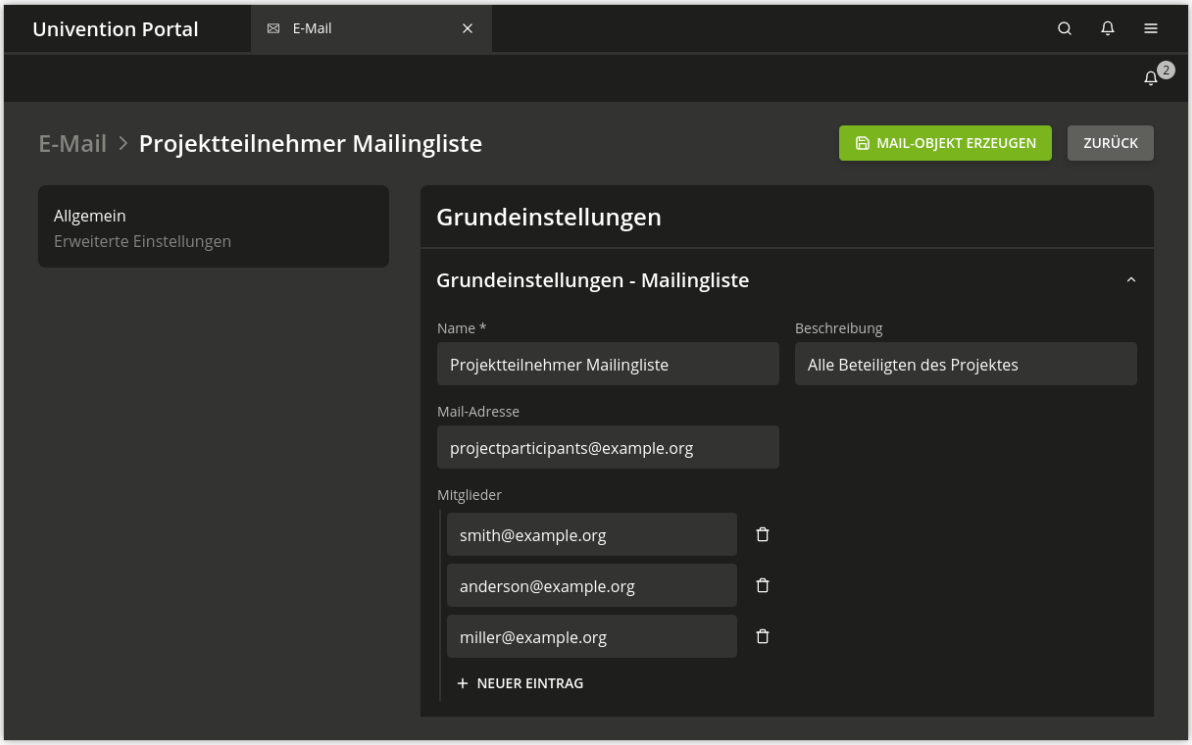


Abb. 14.1: Einrichtung einer Mailingliste

14.2.4 Verwaltung von Mailgruppen

Es besteht die Möglichkeit eine Mailgruppe zu bilden: Dabei wird einer Benutzer-Gruppe eine E-Mail-Adresse zugewiesen. E-Mails an diese Adresse werden dann allen Gruppenmitgliedern an ihre primäre E-Mail-Adresse zugestellt.

Mailgruppen werden im UMC-Modul *Gruppen* verwaltet (siehe auch *Gruppenverwaltung* (Seite 139)).

Die E-Mail-Adresse der Mailgruppe wird im Eingabefeld *Mail-Adresse* unter *Erweiterte Einstellungen* festgelegt. Der Domänenteil der Adresse muss einer der verwalteten Mail-Domänen entsprechen.

In der Grundeinstellung kann jeder an die Mailgruppe schreiben. Um Missbrauch zu verhindern, besteht die Möglichkeit den Senderkreis einzuschränken. Dazu muss die Univention Configuration Registry Variable `mail/postfix/policy/listfilter` (Seite 312) auf dem Mailserver auf `yes` gesetzt und Postfix neu gestartet werden.

Unter *Erweiterte Einstellungen* können *Benutzer, die berechtigt sind, E-Mails an diese Gruppe zu versenden* und *Gruppen, die berechtigt sind, E-Mails an diese Gruppe zu versenden* festgelegt werden. Ist hier ein Feld gesetzt, ist das Senden nur den berechtigten Nutzern/Gruppen erlaubt.

14.2.5 Verwaltung von globalen IMAP-Ordnern

Ein gemeinsamer Zugriff auf E-Mails ist in vielen Arbeitsgruppen die Grundlage der Zusammenarbeit. Mit UCS können Benutzer sehr einfach Ordner in Ihren eigenen Postfächern anlegen und Berechtigungen vergeben, so dass es weiteren Benutzern gestattet ist, E-Mails in diesen Ordnern zu lesen oder weitere E-Mails in diesen Ordnern abzulegen.

Alternativ können eigene IMAP-Ordner für Benutzer oder Benutzergruppen freigegeben werden. Ein solcher Ordner wird als globaler IMAP-Ordner bezeichnet. Globale IMAP-Ordner werden im UMC-Modul *Mail* mit dem Objekttyp *Mail-Ordner (IMAP)* verwaltet.

Globale IMAP-Ordner können nicht umbenannt werden. Die Univention Configuration Registry Variable `mail/dovecot/mailbox/rename` (Seite 311) kommt daher nicht zur Anwendung. Nur wenn `mail/dovecot/mailbox/delete` (Seite 311) auf `yes` gesetzt ist (Standard ist `no`), wird ein globaler IMAP-Ordner beim Löschen im UMC-Modul *Mail* auch tatsächlich von der Festplatte gelöscht.

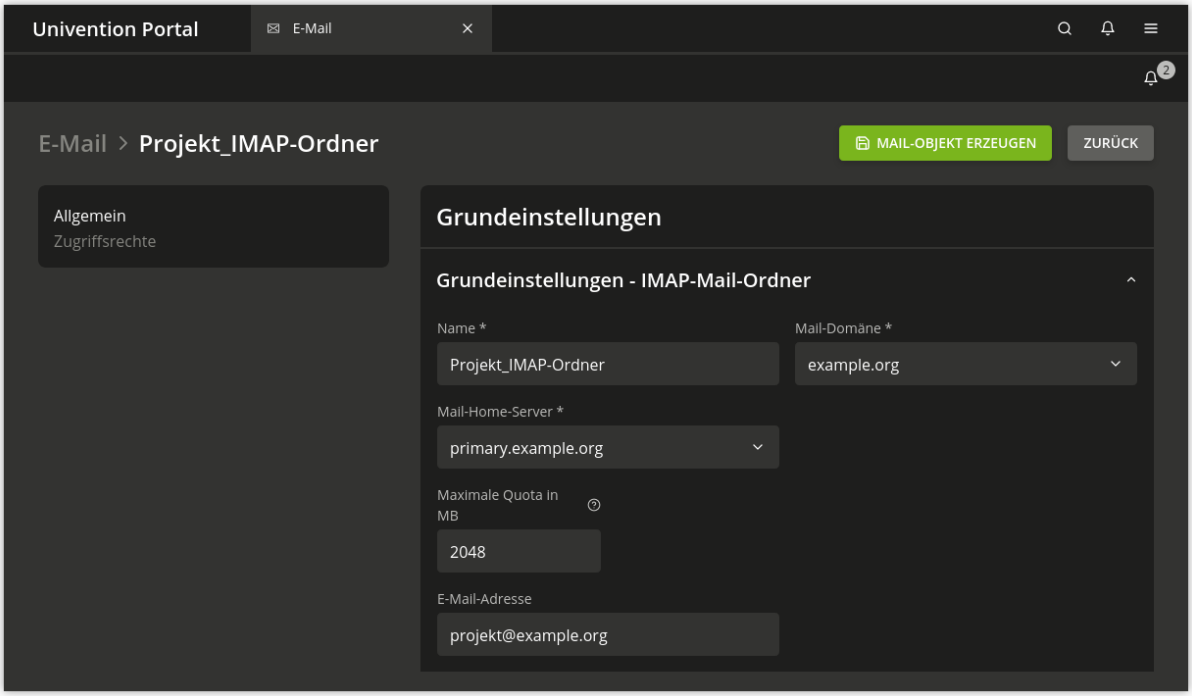


Abb. 14.2: Einrichtung eines globalen IMAP-Ordners

Globaler IMAP-Ordner - Reiter Allgemein

Tab. 14.1: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Der Name, unter dem der IMAP-Ordner im E-Mail-Client verfügbar ist. Der Name unterscheidet sich je nach dem, ob eine E-Mail-Adresse konfiguriert wird (siehe Zeile „Mail-Adresse“ unten) oder nicht. Wird keine Mail-Adresse konfiguriert, erscheint der IMAP-Ordner im Client als `name@domain/INBOX`. Wird eine Mail-Adresse verwendet, wird der Name die Form `shared/name@domain` haben.
Mail-Domäne (*)	Jeder globale IMAP-Ordner ist einer Mail-Domäne zugeordnet. Die Verwaltung der Domänen ist in *Verwaltung von Mail-Domänen* (Seite 272) dokumentiert.
Mail Home Server (*)	Ein IMAP-Ordner ist einem Mail Home Server zugeordnet. Weitere Hinweise finden sich in *Verteilung einer Installation auf mehrere Mailserver* (Seite 284).
Quota in MB	Mit dieser Einstellung kann die maximale Gesamtgröße aller E-Mails in diesem Ordner festgelegt werden.
E-Mailadresse	Hier kann eine E-Mail-Adresse angegeben werden, durch die E-Mails direkt an den IMAP-Ordner gesendet werden können. Ist hier keine Adresse gesetzt, so kann nur aus E-Mail-Clients heraus in den Ordner geschrieben werden. Der Domänenanteil der E-Mail-Adresse muss im UMC-Modul *E-Mail* registriert sein (siehe *Verwaltung von Mail-Domänen* (Seite 272)).

Globale IMAP-Ordner - Reiter Zugriffsrechte

Tab. 14.2: Reiter *Zugriffsrechte*

Attribut	Beschreibung
Name (*)	Hier können Zugriffsberechtigungen auf Basis von Benutzern oder Gruppen vergeben werden. Benutzer werden mit Ihrem Benutzernamen eingetragen; als Gruppen werden die im UMC-Modul *Gruppen* angelegten Gruppen verwendet. Die Zugriffsrechte haben folgende Auswirkungen für einzelne Benutzer oder Mitglieder der angegebenen Gruppe: **Keine** Es ist kein Zugriff möglich. Der Ordner wird nicht in der Ordnerliste angezeigt. **Lesen** Es darf nur lesend auf bestehende Einträge zugegriffen werden. **Anhängen** Bestehende Einträge dürfen nicht verändert werden, nur neue Einträge erzeugt werden. **Schreiben** Neue Einträge in diesem Ordner anlegen, bestehende verändern oder bestehende löschen ist erlaubt. **Senden** Eine E-Mail an diesen Ordner als Empfänger senden ist zugelassen. Dies wird nicht von jedem Client unterstützt. **Alles** Umfasst alle Berechtigungen von *Schreiben* und erlaubt zusätzlich das Ändern von Zugriffsrechten.

14.2.6 Mail-Quota

Die Größe der Benutzerpostfächer kann über Mail-Quotas eingeschränkt werden, bei deren Erreichen vom Mailserver keine weiteren E-Mails für das Postfach angenommen werden, bis der Benutzer alte Mails aus seinem Konto entfernt hat.

Die Grenze wird in Megabytes im Feld *Mail-Quota* festgelegt, die unter *Erweiterte Einstellungen ▸ Mail* verwaltet wird. Der Standardwert ist `0` und bedeutet, dass keine Beschränkung aktiv ist. Für das Zuweisen einer Quota an mehrere Benutzer auf einmal, kann der Mehrfachbearbeitungsmodus von UMC-Modulen verwendet werden, siehe *Bearbeiten von Objekten* (Seite 75).

Der Benutzer kann ab einer bestimmten erreichten Postfachgröße gewarnt werden und erhält dann eine Mail mit dem Hinweis, dass seine Speicherressourcen nahezu ausgeschöpft sind. Der Administrator kann den Schwellwert in Prozent, den Betreff der Nachricht und ihren Inhalt angeben:

- In der Univention Configuration Registry Variable *mail/dovecot/quota/warning/text* (Seite 312) kann der Schwellwert konfiguriert werden, ab dem eine Warnmeldung ausgegeben werden soll, zum Beispiel: `mail/dovecot/quota/warning/text/`*`PROZENT=TEXT`*

  `PROZENT` muss als Zahl zwischen 0 und 100 ohne Prozentzeichen angegeben werden.

  `TEXT` ist der Inhalt der E-Mail. Wenn `TEXT` die Zeichenkette `$PERCENT` enthält, wird diese in der E-Mail mit dem überschrittenen Wert ersetzt.

  Der Wert der Univention Configuration Registry Variable *mail/dovecot/quota/warning/subject* (Seite 311) wird als Betreff der E-Mails verwendet.

- Bei der Installation des Mail-Server-Paketes werden Betreff und zwei Warn-Nachrichten automatisch konfiguriert:

  – *mail/dovecot/quota/warning/subject* (Seite 311) wird gesetzt auf `Quota-Warning`

- `mail/dovecot/quota/warning/text/80` wird gesetzt auf `Your mailbox has filled up to over $PERCENT%.`
- `mail/dovecot/quota/warning/text/95` wird gesetzt auf `Attention: Your mailbox has already filled up to over $PERCENT%. Please delete some messages or contact the administrator.`

14.3 Spamerkennung und -filterung

Unerwünschte und nicht angeforderte E-Mails werden als Spam bezeichnet. Zur automatisierten Erkennung solcher E-Mails integriert UCS die Software SpamAssassin und Postgrey. SpamAssassin versucht anhand von Heuristiken über Herkunft, Form und Inhalt einer E-Mail zu erkennen, ob sie erwünscht ist oder nicht. Postgrey ist ein Policy Server für Postfix, der „Greylisting“ implementiert. Greylisting ist eine Spam-Erkennungsmethode die E-Mail beim ersten Zustellversuch eines externen Servers ablehnt. Mailserver von Spamversendern unternehmen häufig keinen zweiten Zustellversuch, während legitime Server dies tun. Die Integration erfolgt über die Pakete **univention-spamassassin** und **univention-postgrey**, die bei der Einrichtung des Mailserver-Pakets automatisch eingerichtet werden.

SpamAssassin arbeitet mit einem Punktesystem, das mit steigender Punktzahl eine höhere Wahrscheinlichkeit für Spam ausdrückt. Punkte werden nach verschiedenen Kriterien vergeben, die beispielsweise auf Schlagworte innerhalb der E-Mail oder fehlerhafte Codierungen ansprechen. In der Grundeinstellung werden nur Mails bis zu einer Größe von 300 Kilobyte geprüft. Dies kann mit der Univention Configuration Registry Variable *mail/antispam/bodysizelimit* (Seite 310) konfiguriert werden.

E-Mails, die als Spam klassifiziert wurden - also eine bestimmte Anzahl Punkte überschreiten - werden bei der Auslieferung durch Dovecot nicht im Posteingang des Empfängers, sondern im darunter liegenden Ordner *Spam* abgelegt. Der Name des Ordners kann mit der Univention Configuration Registry Variable *mail/dovecot/folder/Spam* (Seite 310) konfiguriert werden. Die Filterung erfolgt durch ein Sieve-Skript, das beim Anlegen des IMAP-Postfachs eines Benutzers automatisch generiert wird.

Der in die Sieve-Skripte eingetragene Schwellwert, ab der E-Mails als Spam deklariert werden, ist mit der Univention Configuration Registry Variable *mail/antispam/requiredhits* (Seite 310) konfigurierbar. Die Voreinstellung (`5`) muss in der Regel nicht angepasst werden. Je nach Erfahrung im eigenen Umfeld kann dieser Wert aber auch niedriger angesetzt werden. Es muss dann jedoch mit mehr E-Mails gerechnet werden, die fälschlich als Spam erkannt wurden. Die Änderung des Schwellwerts wirkt sich nicht auf bestehende Benutzer aus.

Zusätzlich gibt es die Möglichkeit, E-Mails mit einem Bayes-Klassifikator bewerten zu lassen. Dieser vergleicht eine eingehende E-Mail mit statistischen Daten, die er aus bereits verarbeiteten E-Mails gewonnen hat und kann so seine Bewertung an die Mailgewohnheiten anpassen. Die Bayes-Klassifizierung wird vom Benutzer selbst gesteuert, in dem nicht vom System aber vom Benutzer als Spam erkannte E-Mails in den Unterordner *Spam* verschoben und eine Auswahl legitimer Mails in den Unterordner *Ham* (*mail/dovecot/folder/ham* (Seite 310)) kopiert werden. Diese Ordner werden täglich ausgewertet und noch nicht erfasste oder bisher falsch klassifizierte Daten in einer gemeinsamen Datenbank erfasst. Diese Auswertung ist in der Grundeinstellung aktiviert und kann mit der Univention Configuration Registry Variable *mail/antispam/learndaily* (Seite 310) konfiguriert werden.

Die Spam-Filterung kann durch Setzen der Univention Configuration Registry Variable *mail/antivir/spam* (Seite 310) auf `no` deaktiviert werden. Bei Änderungen an Univention Configuration Registry-Variablen, die die Spamerkennung betreffen, muss der AMaViS-Dienst und Postfix neu gestartet werden.

14.4 Viren- und Malwareerkennung

Die UCS-Maildienste integrieren eine Viren- und Malwareerkennung über das Paket **univention-anti-vir-mail**, das bei der Einrichtung des Mailserver-Pakets automatisch eingerichtet wird. Der Virenscan kann mit der Univention Configuration Registry Variable *mail/antivir* (Seite 310) deaktiviert werden.

Alle ein- und ausgehenden E-Mails werden auf Viren geprüft. Wird ein Virus erkannt, wird die E-Mail unter Quarantäne gestellt, d.h. auf dem Server unerreichbar für den Benutzer abgelegt. Der ursprüngliche Empfänger erhält eine Benachrichtigung per E-Mail über diese Maßnahme. Bei Bedarf kann der Administrator die E-Mail aus dem Verzeichnis `/var/lib/amavis/virusmails/` wiederherstellen oder löschen. Eine automatische Löschung erfolgt nicht.

Die Software **AMaViSd-new** dient als Schnittstelle zwischen dem Mailserver und verschiedenen Virenscannern. Der freie Virenscanner ClamAV ist im Paket enthalten und nach der Installation sofort einsatzbereit. Die für die Virenerkennung nötigen Signaturen werden automatisch und kostenfrei durch den Freshclam-Dienst bezogen und aktualisiert.

Alternativ oder zusätzlich können andere Virenscanner in AMaViS eingebunden werden. Nach Änderungen an der AMaViS- oder ClamAV-Konfiguration müssen Postfix und AMaViS neu gestartet werden.

14.5 Identifikation von Spam Quellen mit DNS basierten Blackhole Listen

Eine weitere Möglichkeit gegen Spam vorzugehen ist die Verwendung von *DNS-based Blackhole List* (DNSBL) oder *Real-time Blackhole Lists* (RBL). DNSBL sind Listen von IP Adressen, von denen der Betreiber denkt, dass sie (potentiell) Quellen von Spam sind. Die Listen werden per DNS abgefragt. Ist dem DNS-Server die IP des sendenden E-Mail-Servers bekannt, so wird die Nachricht abgelehnt. Der Check einer IP-Adresse ist schnell und vergleichsweise ressourcenschonend. Er findet *vor* dem Annehmen der Nachricht statt. Erst nach dem Empfang findet die aufwändige Inhaltsüberprüfung mit SpamAssassin und Anti-Virus statt. Postfix hat eine eingebaute Unterstützung für DNSBLs[57].

Im Internet existieren DNSBL von verschiedenen Projekten und Firmen. Bitte informieren Sie sich auf deren Webseiten über Konditionen und Preise.

Um DNSBL mit Postfix zu verwenden, muss die Univention Configuration Registry Variable *mail/postfix/smtpd/restrictions/recipient* (Seite 312) mit einem Schlüssel-Wert-Paar *SEQUENCE=RULE* gesetzt werden: `mail/postfix/smtpd/restrictions/recipient/`*SEQUENCE=RULE*.

Mit ihr können Empfangsbeschränkungen über die Postfix-Option `smtpd_recipient_restrictions` konfiguriert werden (siehe Postfix Einstellung smtpd_recipient_restrictions[58]). Die Sequenznummer dient der alphanumerisch Sortierung mehrerer Regeln, über die die Reihenfolge beeinflusst werden kann.

Tipp: Existierende `smtpd_recipient_restrictions` Regeln können wie folgt aufgelistet werden:

```
$ ucr search --brief mail/postfix/smtpd/restrictions/recipient
```

In einer unveränderten Univention Corporate Server Postfix Installation sollten die DNSBL am Ende der `smtpd_recipient_restrictions` Regeln angehängt werden. Zum Beispiel:

```
$ ucr set mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client ix.dnsbl.
↪manitu.net"
```

[57] http://www.postfix.org/postconf.5.html#reject_rbl_client
[58] http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions

14.6 Integration von Fetchmail zum Abrufen von Mail von externen Postfächern

Im Regelfall nimmt der UCS-Maildienst Mails für die Benutzer der UCS-Domäne direkt über SMTP entgegen. UCS bietet zusätzlich eine optionale Integration der Software Fetchmail zum Abrufen von Emails von externen POP3 oder IMAP-Postfächern.

Fetchmail kann über das Univention App Center installiert werden; dort muss die Applikation **`Fetchmail`** ausgewählt werden und auf *Installieren* geklickt werden.

Nach der Installation stellen die Reiter *Erweiterte Einstellungen ▸ Mailabruf von externen Servern (Single)* und *Erweiterte Einstellungen ▸ Mailabruf von externen Servern (Multi)* zusätzliche Eingabefelder bereit. Verwenden Sie diese, um den Abruf von Mails von externen Servern zu konfigurieren.

Fetchmail liefert Mails zu den Posteingängen der jeweiligen Benutzer. Der Account des Benutzers muss dafür über eine primäre E-Mail-Adresse verfügen. Vor der Verwendung von *Multidrop-Konfigurationen* lesen Sie bitte THE USE AND ABUSE OF MULTIDROP MAILBOXES[59].

Der Abruf erfolgt alle zwanzig Minuten sobald mindestens ein Postfach für den Abruf konfiguriert wurde. Nach der initialen Konfiguration eines Benutzers muss Fetchmail im UMC-Modul *Systemdienste* gestartet werden. Dort kann der Start des Dienstes auch deaktiviert werden (alternativ durch Setzen der Univention Configuration Registry Variable *`fetchmail/autostart`* (Seite 305) auf `false`).

Tab. 14.3: Reiter *Mailabruf von externen Servern (Single)*

Attribut	Beschreibung
Benutzername	Der Benutzername für die Verbindung zum Mailserver.
Passwort	Das Passwort für die Verbindung zum Mailserver.
Protokoll	Das Protokoll, welches Fetchmail zum Abrufen von Mails verwendet. Wählen Sie entweder `IMAP` oder `POP3`.
Externer Mailserver	Der Name des Mailservers, den Fetchmail verwendet, um Mails abzurufen.
SSL verwenden	Diese Option aktiviert einen verschlüsselten Abruf von Mails. Dies muss ebenfalls vom Mailserver unterstützt werden.
Mails auf dem externen Server nicht löschen	In der Grundeinstellung löscht Fetchmail die abgerufenen Mails nach deren Übertragung vom externen Server. Um die Mails auf dem externen Server zu behalten, diese Option aktivieren.

[59] https://www.fetchmail.info/fetchmail-man.html#the-use-and-abuse-of-multidrop-mailboxes

Tab. 14.4: Reiter *Mailabruf von externen Servern (Multi)*

Attribut	Beschreibung
Benutzername	Der Benutzername für die Verbindung zum Mailserver.
Passwort	Das Passwort für die Verbindung zum Mailserver.
Protokoll	Das Protokoll, welches Fetchmail zum Abrufen von Mails verwendet. Wählen Sie entweder `IMAP` oder `POP3`.
Externer Mailserver	Der Name des Mailservers, den Fetchmail verwendet, um Mails abzurufen.
Lokale Domänennamen	Eine durch Leerzeichen getrennte Liste lokaler Domänennamen. Feld leer lassen, um alle lokalen Domänen zu verwenden.
Virtuelle *Qmail* Präfix	Fetchmail entfernt den angegebenen Präfix von der Mailadresse aus dem Header, welche mit der Option *Envelope-Header* angegeben ist. Wenn dieser Wert beispielsweise `example-prefix-` ist und Fetchmail eine Mail abruft, in deren Header `example-prefix-info@remotedomain.com` vorkommt, leitet Fetchmail die Mail an `info@localdomain.com` weiter.
Envelope-Header	Ändert den Wert des Headers, in welchem Fetchmail eine Kopie der *Envelope-Adresse* erwartet. Fetchmail verwendet diesen zur Umleitung von E-Mails.
SSL verwenden	Diese Option aktiviert einen verschlüsselten Abruf von Mails. Dies muss ebenfalls vom Mailserver unterstützt werden.
Mails auf dem externen Server nicht löschen	In der Grundeinstellung löscht Fetchmail die abgerufenen Mails nach deren Übertragung vom externen Server. Um die Mails auf dem externen Server zu behalten, diese Option aktivieren.

14.7 Konfiguration des Mailservers

Dieser Abschnitt beschreibt die Konfiguration des Mailservers **Postfix** in UCS.

14.7.1 Konfiguration eines Relay-Hosts für den Mailversand

Standardmäßig stellt **Postfix** eine direkte SMTP-Verbindung zu dem für die Domain zuständigen Mailserver her, wenn es eine E-Mail an eine nicht lokale Adresse sendet.

Alternativ dazu kann **Postfix** einen Mail-Relay Server verwenden. Dabei handelt es sich um einen Server, der E-Mails empfängt und deren Transport übernimmt. Administratoren können diese Art von Mail-Relay Servern verwenden, z. B. solche, die von der Firmenzentrale oder dem Internet-Provider bereitgestellt werden.

Um einen Relayhost einzurichten, geben Sie ihn als vollqualifizierten Domänennamen (FQDN) in der Univention Configuration Registry Variable *mail/relayhost* (Seite 312) an.

Beispiele

- `ucr set mail/relayhost="mx01.example.com"`

  Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port `25`.

- `ucr set mail/relayhost="mx01.example.com:587"`

  Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port `587`.

Postfix ermittelt die tatsächliche Zieladresse des Relay Mailservers durch Abfrage des MX/SRV Eintrags im DNS. Um die MX Abfrage zu deaktivieren, verwenden Sie das Format `[FQDN-Relay-Host]`, wie in den folgenden Beispielen zu sehen:

- `ucr set mail/relayhost="[mx01.example.com]"`

  Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port `25`.

- `ucr set mail/relayhost="[mx01.example.com]:587"`

Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port `587`.

Wenn für das Senden eine Authentifizierung auf dem Relayhost erforderlich ist, setzen Sie die Univention Configuration Registry Variable *mail/relayauth* (Seite 312) auf `yes` und bearbeiten Sie die Datei `/etc/postfix/smtp_auth`. Geben Sie in dieser Datei den FQDN des Relayhost, den Benutzernamen und das Passwort in einer Zeile in folgendem Format ein: *FQDN Relayhost Benutzername*`:`*Passwort*. Der Teil für *FQDN Relayhost* muss genau wie der Wert von *mail/relayhost* (Seite 312) aussehen.

Beispiele

- `mx01.example.com:587 outgoing-username@example.com:verySecretPassword`
- `[mx01.example.com]:587 outgoing-username@example.com:verySecretPassword` mit ausgeschalteter MX Abfrage

Um die Änderungen in **Postfix** zu übernehmen, führen Sie die folgenden Befehle aus:

1. Aktualisieren Sie die Authentifizierungszuordnung:

```
$ postmap /etc/postfix/smtp_auth
```

2. Wenn Sie *mail/relayauth* (Seite 312) geändert haben, müssen Sie die Datei für die TLS-Richtlinien aktualisieren:

```
$ postmap /etc/postfix/tls_policy
```

3. Wenn Sie *mail/relayhost* (Seite 312) geändert haben, müssen Sie dem Mailserver sagen, dass er die Konfiguration neu laden soll:

```
$ service postfix reload
```

Bemerkung: Um eine verschlüsselte Verbindung bei Verwendung eines Relay-Hosts zu gewährleisten, müssen Sie die **Postfix**-Konfigurationsoption `smtp_tls_security_level` auf `encrypt` setzen.

Univention Corporate Server setzt diese Option automatisch, wenn die Univention Configuration Registry Variablen *mail/relayhost* (Seite 312) und *mail/relayauth* (Seite 312) den Wert `yes` haben und wenn *mail/postfix/tls/client/level* (Seite 312) nicht den Wert `none` hat.

Siehe auch:

***postconf(5)* - Manual Seite für `postconf` - Postfix Konfigurationsparameter**
für eine Referenz der Konfigurationswerte relayhost[60], und smtp_sasl_password_maps[61].

14.7.2 Konfiguration der maximalen E-Mailgröße

Mit der Univention Configuration Registry Variable *mail/messagesizelimit* (Seite 312) kann die maximale Größe in Byte für ein- und ausgehende E-Mails festgelegt werden. Die voreingestellte Maximalgröße beträgt `10240000` Byte. Nach Änderung der Einstellung muss Postfix neu gestartet werden. Wird `0` als Wert konfiguriert, so wird die Begrenzung aufgehoben. Es ist zu beachten, dass Emailanhänge durch die *base64*-Kodierung um ca. ein Drittel vergrössert werden.

[60] https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#relayhost_(default:_empty)
[61] https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#smtp_sasl_password_maps_(default:_empty)

14.7.3 Konfiguration einer Blindkopie zur Anbindung von E-Mail-Archivierungslösungen

Wird die Univention Configuration Registry Variable *mail/archivefolder* (Seite 310) auf eine E-Mail-Adresse gesetzt, sendet Postfix eine Blindkopie aller ein- und ausgehenden E-Mails an diese Adresse. So kann eine Archivierung aller E-Mails erreicht werden. Die E-Mail-Adresse muss bereits existieren. Sie kann entweder eine in Univention Corporate Server registrierte E-Mail-Adresse eines Benutzers sein, oder von einem externen Dienst bereitgestellt werden. Standardmäßig ist die Variable nicht gesetzt.

Anschließend muss Postfix neu gestartet werden.

14.7.4 Konfiguration von Softbounces

Bei einer Reihe von Fehlersituationen (z.B. bei nicht vorhandenen Benutzern) kann es zu einem Bounce der betroffenen Mail kommen, d.h. die Mail wird an den Absender zurückgesendet. Mit dem Setzen der Univention Configuration Registry Variable *mail/postfix/softbounce* (Seite 312) auf `yes` werden Mails nie mit einem Bounce zurückgesendet, sondern immer weiterhin in der Queue vorgehalten. Diese Einstellung ist insbesondere für Konfigurationsarbeiten am Mailserver sehr nützlich.

14.7.5 Konfiguration der SMTP Ports

Auf einem Univention Corporate Server Mailserver ist Postfix so konfiguriert, dass es auf Verbindungen an drei Ports lauscht:

Port 25 - SMTP
: Port 25 (`SMTP`) sollte nur von anderen Mailservern verwendet werden. Standardmäßig ist die Authentifikation an diesem Port deaktiviert. Wenn das Einliefern von E-Mails an Port 25 erlaubt werden soll, kann die Univention Configuration Registry Variable *mail/postfix/mastercf/options/smtp/smtpd_sasl_auth_enable* (Seite 312) auf `yes` gesetzt werden.

Port 465 - SMTPS
: Port 465 (`SMTPS`) erlaubt die Authentifikation gegenüber dem Mailserver und das Einliefern von E-Mails über eine mit SSL verschlüsselte Verbindung. `SMTPS` wurde zugunsten von Port 587 als veraltet erklärt, wird jedoch für Altsysteme aktiviert gelassen.

Port 587 - Submission
: Port 587 (`Submission`) erlaubt die Authentifikation gegenüber dem Mailserver und das Einliefern von E-Mails über eine TLS-verschlüsselte Verbindung. Die Verwendung von STARTTLS wird erzwungen.

Der `Submission`-Port sollte von E-Mail-Clients bevorzugt verwendet werden. Die Verwendung der Ports 25 und 465 zur Einlieferung von E-Mails ist überholt.

14.7.6 Konfiguration zusätzlicher Prüfungen

Bei der Verwendung eines Mailservers, der direkt vom Internet aus erreichbar ist, besteht immer die Gefahr, dass Versender von Spam oder defekte Mailserver kontinuierlich versuchen, auf dem UCS-System ungewollte Mails (z.B. Spam) abzuliefern.

Um die Last des Mailservers für solche Fälle zu reduzieren, bringt Postfix einen eigenen Dienst mit dem Namen **postscreen** mit, der Postfix vorgeschaltet wird und die eingehenden SMTP-Verbindungen annimmt. Mit diesen Verbindungen werden zunächst einige leichtgewichtige Tests durchgeführt. Ist das Ergebnis positiv, wird die Verbindung an Postfix durchgereicht. Im negativen Fall wird die SMTP-Verbindung beendet und somit die eingehende Mail abgelehnt, bevor sie im Verantwortungsbereich des UCS Mailservers angekommen ist.

In der Standardeinstellung ist **postscreen** nicht aktiv. Durch das Setzen der Univention Configuration Registry Variable *mail/postfix/postscreen/enabled* (Seite 312) auf den Wert `yes` kann **postscreen** aktiviert werden.

Über diverse UCR-Variablen mit dem Präfix *mail/postfix/postscreen/* (Seite 312) können weitere Einstellungen vorgenommen werden. Eine Liste der UCR-Variablen nebst Beschreibungen können z.B. auf der Kommandozeile über folgenden Befehl abgerufen werden:

```
$ ucr search --verbose mail/postfix/postscreen/
```

Bemerkung: Nach jeder Änderung einer UCR-Variable für **postscreen** sollte die Konfiguration von Postfix und **postscreen** neu geladen werden, was über den Befehl **systemctl reload postfix** ausgelöst werden kann.

14.7.7 Eigene Anpassung der Postfix Konfiguration

Die Konfiguration von Postfix, welche sich in der Datei `/etc/postfix/main.cf` befindet, wird über Univention Configuration Registry-Variablen definiert. Eine Erweiterung der Konfiguration, die über die vorhandenen Univention Configuration Registry-Variablen hinaus geht, ist ebenso möglich.

Existiert die Datei `/etc/postfix/main.cf.local`, so wird ihr Inhalt an die Datei `main.cf` angehängt. Damit Änderungen an `main.cf.local` nach `main.cf` übernommen werden, muss der folgende Befehl ausgeführt werden:

```
$ ucr commit /etc/postfix/main.cf
```

Zum Übernehmen der Änderungen durch den Postfix Dienst muss dieser neu geladen werden:

```
$ systemctl reload postfix
```

Wird in der Datei `main.cf.local` eine Postfix Variable gesetzt, die zuvor auch in `main.cf` gesetzt wurde, so schreibt Postfix eine Warnung in die Logdatei `/var/log/mail.log`.

Bemerkung: Wenn das Verhalten des E-Mail-Servers nicht der Erwartung entspricht, sollten zuerst die Einstellungen, die durch `main.cf.local` aktiviert wurden, rückgängig gemacht werden. Dazu muss die Datei umbenannt oder ihr Inhalt auskommentiert werden. Im Anschluss müssen die beiden oben genannten Kommandos ausgeführt werden. Die Konfiguration entspricht dann wieder der Standardkonfiguration von UCS.

14.7.8 Konfiguration des Alias Expansion Limits

Werden E-Mails an einer Gruppe gesendet, die wiederum andere Gruppen enthält, kann es passieren, dass diese E-Mails nicht akzeptiert werden. Das liegt daran, dass Postfix durch eine Virtual Alias Expansion versucht, die Anzahl der ursprünglichen Empfänger entsprechend zu erweitern. Diese Anzahl wird standardmäßig auf 1000 Nutzer begrenzt und kann daher zu gering sein.

Um den Wert auf beispielsweise 5000 Nutzer zu erhöhen, muss die folgende Zeile in `/etc/postfix/main.cf.local` hinzugefügt oder angepasst werden:

```
virtual_alias_expansion_limit = 5000
```

Danach muss Postfix neugestartet werden:

```
$ systemctl restart postfix
```

14.7.9 Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten

Das Postfach eines Benutzers ist mit der primären E-Mail-Adresse verknüpft und nicht mit dem Benutzernamen. Mit der Univention Configuration Registry Variable *mail/dovecot/mailbox/rename* (Seite 311) kann das Verhalten bei der Änderung der primären E-Mail-Adresse konfiguriert werden:

- Ist die Variable auf `yes` gesetzt, wird das IMAP-Postfach des Benutzers umbenannt. Dies ist seit UCS 3.0 die Standardeinstellung.
- Bei der Einstellung `no`, sind nach dem Ändern der primären E-Mail-Adresse eines Benutzers seine bisherigen E-Mails nicht mehr erreichbar! Wird einem anderen Benutzer eine ehemals vergebene primäre E-Mail-Adresse zugewiesen, bekommt dieser Zugriff auf die alte IMAP-Struktur dieses Postfachs.

Mit der Univention Configuration Registry Variable *mail/dovecot/mailbox/delete* (Seite 311) kann konfiguriert werden, ob IMAP-Postfächer automatisch gelöscht werden sollen. Der Wert `yes` aktiviert die Löschung des betroffenen IMAP-Postfachs bei folgenden Aktionen:

- dem Löschen des Benutzerkontos
- dem Entfernen der primären Mailadresse von einem Benutzerkonto
- dem Ändern des Mail Home Servers auf ein anderes System

In der Grundeinstellung (`no`) bleiben die Postfächer bei diesen Aktionen erhalten, wenn eine der obigen Aktionen durchgeführt wird.

Aus der Kombination der beiden Variablen ergeben sich folgende vier Fälle, wenn E-Mail-Adressen geändert werden:

Tab. 14.5: Umbenennung von E-Mail-Adressen

mail/dovecot/mailbox/...	Bedeutung
`rename=yes` und `delete=no` (Standard)	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
`rename=yes` und `delete=yes`	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
`rename=no` und `delete=no`	Eine neue, leere Mailbox wird erzeugt. Die alte bleibt unter dem alten Namen auf der Festplatte erhalten und ist damit vorerst für Benutzer nicht zu erreichen.
`rename=no` und `delete=yes`	Eine neue, leere Mailbox wird erzeugt. Die alte Mailbox wird inklusive aller enthaltenen Mails von der Festplatte gelöscht.

14.7.10 Verteilung einer Installation auf mehrere Mailserver

Das UCS-Mailsystem bietet die Möglichkeit die Benutzer auf mehrere Mailserver zu verteilen. Dazu wird jedem Benutzer ein sogenannter Mail Home Server zugewiesen, auf dem die Maildaten des Benutzers abgelegt werden. Beim Zustellen einer E-Mail wird der zuständige Home Server automatisch aus dem LDAP-Verzeichnis ermittelt.

Es ist zu beachten, dass globale IMAP-Ordner (siehe *Verwaltung von globalen IMAP-Ordnern* (Seite 274)) einem Mail Home Server zugeordnet sind.

Beim Ändern des Mail Home Servers eines Benutzers werden dessen E-Mails *nicht* automatisch auf den neuen Server verschoben.

14.7.11 Mailserver-Speicher auf NFS

Dovecot unterstützt das Speichern von E-Mails und Index-Dateien auf Cluster-Dateisystemen und NFS. Einige Einstellungen sind jedoch nötig, um Datenverluste in bestimmten Situationen zu vermeiden.

Die folgenden Einstellungen gehen davon aus, dass auf Mailboxen nicht gleichzeitig von mehreren Servern aus zugegriffen wird. Das ist der Fall, wenn jedem Benutzer ein Mail Home Server zugeordnet ist.

- *mail/dovecot/process/mmap_disable* (Seite 311)=yes
- *mail/dovecot/process/dotlock_use_excl* (Seite 311)=yes
- *mail/dovecot/process/mail_fsync* (Seite 311)=always

Um eine bessere Performance zu erreichen, können Index-Dateien statt zusammen mit den Nachrichten im NFS auch auf der lokalen Festplatte gespeichert werden. Sie sind dann unter /var/lib/dovecot/index/ zu finden. Setzen Sie dafür die Univention Configuration Registry Variable *mail/dovecot/location/separate_index* (Seite 311)=yes.

Mit diesen Einstellungen sollte normalerweise alles problemlos funktionieren. Die im Einsatz befindlichen Server- und Client-Systeme sind jedoch so vielfältig, dass hier noch ein paar Hinweise folgen, wie bei Schwierigkeiten weiter vorgegangen werden kann:

- Wenn NFSv2 im Einsatz ist (nicht der Fall, wenn der NFS-Server ein Univention Corporate Server ist), setzen Sie bitte *mail/dovecot/process/dotlock_use_excl* (Seite 311)=no.
- Falls kein lockd eingesetzt wird (nicht der Fall auf Univention Corporate Server-Systemen) oder falls trotz des Einsatzes von lockd Locking-Fehler auftreten, setzen Sie *mail/dovecot/process/lock_method* (Seite 311)=dotlock. Dies verringert die Performance, aber behebt die meisten Locking-bezogenen Probleme.
- Dovecot kann mit *mail/dovecot/process/mail_nfs_storage* (Seite 311)=yes angewiesen werden, wenn nötig, den NFS Cache zu leeren. Dies funktioniert jedoch nicht immer, daher kann es zu sporadischen Fehlern kommen. Das gleiche gilt für das Leeren des NFS-Cache nach dem Schreiben von Index-Dateien: *mail/dovecot/process/mail_nfs_index* (Seite 311)=yes.

Siehe auch:

Mail Location Settings[Seite 285, 62] **in der Dovecot Dokumentation**
für weitere Informationen über Mailbox Orte.

Shared mailboxes[63] **in der Dovecot Dokumentation**
für weitere Informationen über das Teilen von Mailboxen.

NFS[64] **in der Dovecot Dokumentation**
für weitere Informationen über die Verwendung von Dovecot mit NFS.

14.7.12 Beschränkung der Verbindungsanzahl

In der Standardeinstellung in UCS wird Dovecot für jeweils maximal 400 gleichzeitige Verbindungen per IMAP und POP3 ausgeliefert. Diese reichen sicher aus, um 100 gleichzeitig eingeloggte IMAP-Benutzer zu bedienen, unter Umständen deutlich mehr.

Wie viele IMAP-Verbindungen Benutzer gleichzeitig geöffnet haben, hängt von den eingesetzten Clients ab:

- Webmail öffnet nur einzelne, kurzlebige Verbindungen.
- Desktop E-Mail-Programme halten über lange Zeit mehrere Verbindungen offen.
- Mobile Clients halten über lange Zeit wenige Verbindungen offen, aber beenden diese oft nicht von sich aus, so dass sie unnötig lang Ressourcen belegen.

[62] https://doc.dovecot.org/2.3/configuration_manual/mail_location/
[63] https://doc.dovecot.org/2.3/configuration_manual/shared_mailboxes/
[64] https://doc.dovecot.org/2.3/configuration_manual/nfs/

Die Beschränkungen dienen primär dazu, einem Denial-of-Service Angriff durch sehr viele geöffnete Prozesse und Netzwerkverbindungen zu widerstehen.

Um die in diesem Augenblick offenen Verbindungen zu sehen, kann folgender Befehl ausgeführt werden:

```
$ doveadm who
```

Um die Gesamtanzahl auszugeben:

```
$ doveadm who -1 | wc -l
```

Um die Beschränkungen zu verändern, können die Univention Configuration Registry Variablen *mail/dovecot/limits* (Seite 311)*/** angepasst werden. Der Vorgang ist auf Grund des komplexen Zusammenspiels dieser Variablen nur halb automatisch. Die Bedeutung aller Variablen kann in Dovecot Dokumentation: Service configuration[65] nachgelesen werden.

Da bei Dovecot verschiedene Prozesse für Login und Zugriff auf die E-Mail-Dateien zuständig sind, können diese getrennt konfiguriert werden. Zusätzlich wird getrennt konfiguriert, wie viele Verbindungen zu einem Dienst erlaubt sind und wie viele Prozesse für einen Dienst gestartet werden. Durch das Setzen von `mail/dovecot/limits/default_client_limit=3000` würde die Beschränkung für die Anzahl an Verbindungen zu den POP3- und IMAP-Diensten verändert, nicht jedoch für die erlaubte Anzahl an Prozessen. In der Univention Corporate Server Standardeinstellung läuft Dovecot im *High-security mode*: Jede Verbindung wird von einem separaten Login-Prozess betreut. Da standardmäßig nur 400 Prozesse erlaubt sind, können auch nicht mehr Verbindungen geöffnet werden.

Um 3000 Verbindungen von Benutzern zu ihren E-Mails zu erlauben, muss daher eine weitere Univention Configuration Registry Variable gesetzt werden:

```
$ ucr set mail/dovecot/limits/default_client_limit=3000
$ ucr set mail/dovecot/limits/default_process_limit=3000
$ doveadm reload
```

Ein Blick in `/var/log/dovecot.info` offenbart nun eine Warnung:

```
config: Warning: service auth { client_limit=2000 } is lower than required under␣
↪max. load (15000)
config: Warning: service anvil { client_limit=1603 } is lower than required under␣
↪max. load (12003)
```

Die Dienste `auth` (Zuständig für Login und SSL-Verbindungen) sowie `anvil` (Zuständig für Statistiken) haben noch das Standardlimit. Es werden zwar je 3000 POP3- und IMAP-Verbindungen und -Prozesse erlaubt, aber die Anzahl der Prozesse für Login und SSL ist nun zu niedrig um sie alle zu bedienen. Dies wird dazu führen, dass Logins fehlschlagen.

Die hohen Werte kommen dadurch zustande, dass mit `default_client_limit` und `default_process_limit` nicht nur die Beschränkungen von IMAP und POP3 erhöht werden, sondern auch einiger weiterer Dienste wie `lmtp` und `managesieve-login`. Diese Dienste können nun mehr zu überwachende Prozesse starten und theoretisch mehr Authentifizierungen durchführen, wodurch sich die maximale Anzahl gleichzeitiger Verbindungen zu den Diensten `auth` und `anvil` erhöht.

Die Werte für die Dienste müssen nun der Fehlermeldung entsprechend angepasst werden:

```
$ ucr set mail/dovecot/limits/auth/client_limit=15000
$ ucr set mail/dovecot/limits/anvil/client_limit=12003
$ doveadm reload
```

Ein Blick in `/var/log/dovecot.info` offenbart nun noch eine letzte Warnung:

```
master: Warning: fd limit (ulimit -n) is lower than required under max. load (2000
↪< 15000),…
 because of service auth { client_limit }
```

[65] https://doc.dovecot.org/2.3/configuration_manual/service_configuration/

Das vom Linux-Kernel kontrolliere `ulimit` (die erlaubte Anzahl gleichzeitig geöffneter Dateien/Verbindungen pro Prozess) wird nur bei einem Neustart des Dovecot-Dienstes verändert, daher:

```
$ systemctl restart dovecot
```

Nun erscheint keine Fehlermeldung mehr, und IMAP- und POP3-Server akzeptieren nun beide je 3000 Verbindungen.

Univention Corporate Server konfiguriert Dovecot so, dass es standardmäßig im *High-security mode* läuft. In Installationen mit zehntausenden Benutzern kann Dovecot im *High-performance mode* betrieben werden. Der Performance-Leitfaden beschreibt, wie dieser konfiguriert werden kann, siehe *UCS performance guide* [5].

14.8 Konfiguration von Mail-Clients für den Mailserver

Um einen Mail-Client mit dem UCS-Mailserver zu verwenden, wird die Verwendung von IMAP empfohlen. Durch STARTTLS wird bei Verwendung von SMTP (für den Mailversand) und IMAP (für den Mailabruf/-synchronisation) nach einer initialen Aushandlungsphase auf eine TLS-gesicherte Verbindung umgeschaltet. Als Authentifizierungsmethode sollte *Passwort (plain text)* in Verbindung mit *STARTTLS* verwendet werden. Die Benennung der Methode unterscheidet sich je nach Mail-Client. Der folgende Screenshot zeigt exemplarisch die Einrichtung von Mozilla Thunderbird.

Abb. 14.3: Einrichtung von Mozilla Thunderbird

14.9 OX Connector

OX Connector ist eine App im Univention App Center. Sie synchronisiert ausgewählte Benutzer und Gruppen zu **OX App Suite** und entfernten Installation wie zum Beispiel ein OX App Suite bei einem Hosting Anbieter. Seit **OX Connector** Version `2.1.2` und **OX App Suite** Version `7.10.6-ucs4`, integriert der **OX Connector** mit **OX App Suite** aus dem Univention App Center, um Nutzer- und Gruppenkonten zu **OX App Suite** zu synchronisieren.

Warnung: **OX App Suite** Versionen älter als `7.10.6-ucs4` beinhalten ihre eigene Synchronisation. **OX Connector** synchronisiert sich nicht mit diesen Versionen und darf daher nicht mit der separaten App **OX App Suite** aus dem App Center verwendet werden.

Siehe auch:

OX Connector App Dokumentation

Weitere Informationen über den **`OX Connector`** finden Sie in Integration of OX Connector and OX App Suite app[66] in der entsprechenden Dokumentation unter *Univention OX Connector app documentation* [16], verfügbar nur in Englisch.

[66] https://docs.software-univention.de/ox-connector-app/latest/limitations.html#limit-ox-app-suite-app

KAPITEL 15

Infrastruktur-Monitoring

UCS bietet zwei unterschiedliche Lösungen für das Monitoring der Infrastruktur.

Das UCS Dashboard hilft einerseits den Administratoren, schnell den Zustand von Domänen und einzelnen Servern zu erfassen. Zum anderen ist es unter UCS 4.4 mit Nagios möglich, Rechner und Dienste im Hintergrund zu überprüfen und proaktiv eine Benachrichtigung auszulösen, wenn eine Warnstufe erreicht wird. Ab UCS 5.0-2 können Prometheus und Prometheus Alertmanager zur Überwachung eingesetzt. Mit UCS 5.0 wurde die Unterstützung für die Nagios Serverkomponente eingestellt.

15.1 UCS Dashboard

Die **`UCS Dashboard`** App ermöglicht es Administratoren, den Zustand der Domäne und einzelner Server schnell und übersichtlich auf sogenannten Dashboards abzulesen. Die Dashboards sind über einen Web-Browser erreichbar, greifen im Hintergrund auf eine Datenbank zu und liefern kontinuierlich aktualisierte Reports über bestimmte Aspekte der Domäne oder der Server.

15.1.1 Installation

Das UCS Dashboard besteht aus den folgenden Komponenten:

UCS Dashboard
: Die UCS Dashboard App für die Visualisierung von Daten aus der zentralen Datenbank. Diese Komponente basiert auf der Softwarekomponente Grafana[67][1].

UCS Dashboard Database
: Die *UCS Dashboard Database* App, eine Zeitserien-Datenbank für die Speicherung der Metriken. Diese Datenbank wird durch die Software Prometheus bereitgestellt.

UCS Dashboard Client
: Die *UCS Dashboard Client* App für die Bereitstellung der Metriken von Serversystemen. Diese baut auf dem Prometheus Node-Exporter auf.

[67] https://grafana.com/

[1] Die Grafana Labs Marken sind Warenzeichen von Grafana Labs und werden mit Genehmigung von Grafana Labs verwendet. Wir sind weder mit Grafana Labs noch mit seinen Tochtergesellschaften verbunden, noch werden wir von ihnen unterstützt oder gefördert.

Die *UCS Dashboard* App kann über das Univention App Center auf einem Server in der Domäne installiert werden. Die Installation wird nur auf den Systemrollen Primary Directory Node, Backup Directory Node oder Replica Directory Node unterstützt. Die *UCS Dashboard Database* App und die *UCS Dashboard Client* App werden automatisch auf demselben System installiert.

15.1.2 Nutzung

Nach der Installation ist das UCS Dashboard im Portal verlinkt. Alternativ kann es direkt über `https://SERVERNAME-OR-IP/ucs-dashboard/` erreicht werden.

Der Zugriff wird in der Standardeinstellung ausschließlich Benutzern der Gruppe `Domain Admins` (z.B. der Benutzer Administrator) gewährt.

Domain Dashboard

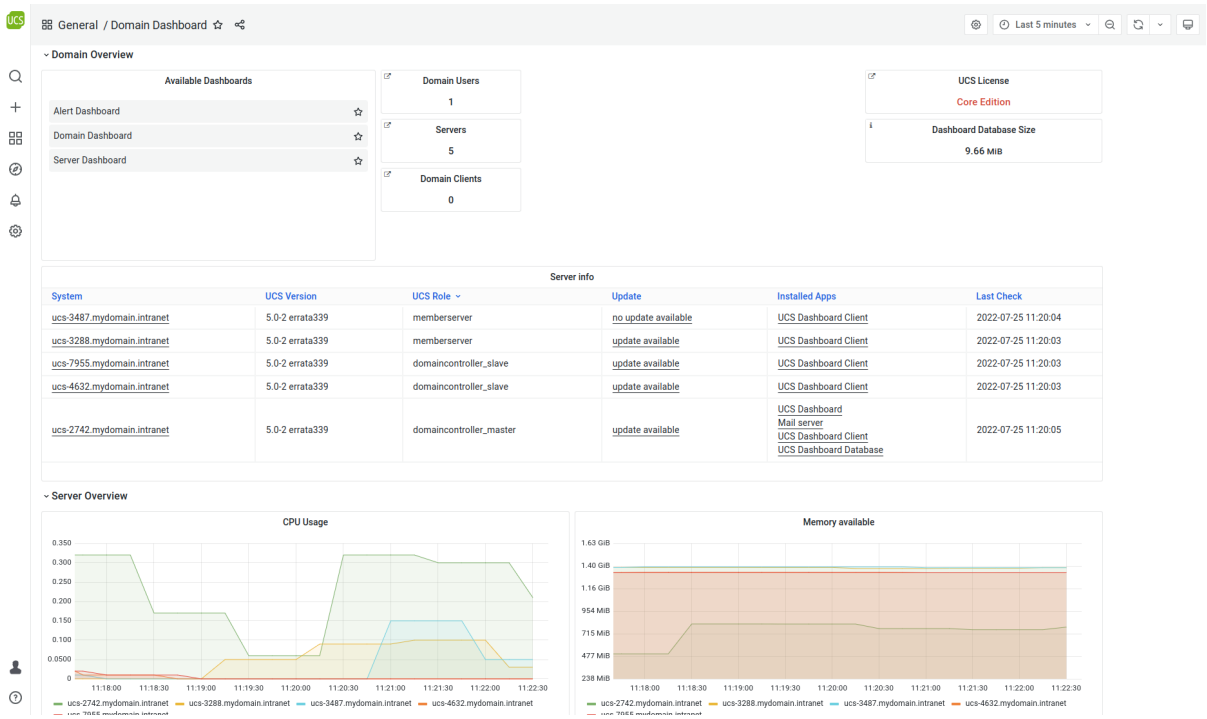


Abb. 15.1: Domain Dashboard

Nach der Anmeldung wird standardmäßig das *Domain Dashboard* geöffnet. Auf diesem Dashboard werden allgemeine Informationen über die Domäne angezeigt, z.B. wie viele Server und wie viele Benutzer in der Umgebung existieren.

Weiter sind auf dem Dashboard, in einer tabellarischen Übersicht, die UCS-Systeme aufgelistet inklusive weiterer Informationen, wie z.B. die Server Rolle, die installierten Apps oder ob ein Update verfügbar ist.

Zusätzlich wird die CPU-Auslastung, Arbeitsspeicherauslastung, der freie Festplattenspeicher und der Status der LDAP-Replikation angezeigt. Dabei werden in den Grafiken jeweils alle Serversysteme angezeigt.

Server Dashboard

Abb. 15.2: Server Dashboard

Standardmäßig wird zusätzlich das *Server Dashboard* eingerichtet. Auf diesem Dashboard sind detaillierte Informationen zu einzelnen Serversystemen aufgelistet, wie z.B. die CPU- oder Speicherauslastung oder der Netzwerkdurchsatz.

Die Server können im Dropdown *server* ausgewählt werden. Anschließend werden die Grafiken entsprechend aktualisiert.

Alert Dashboard

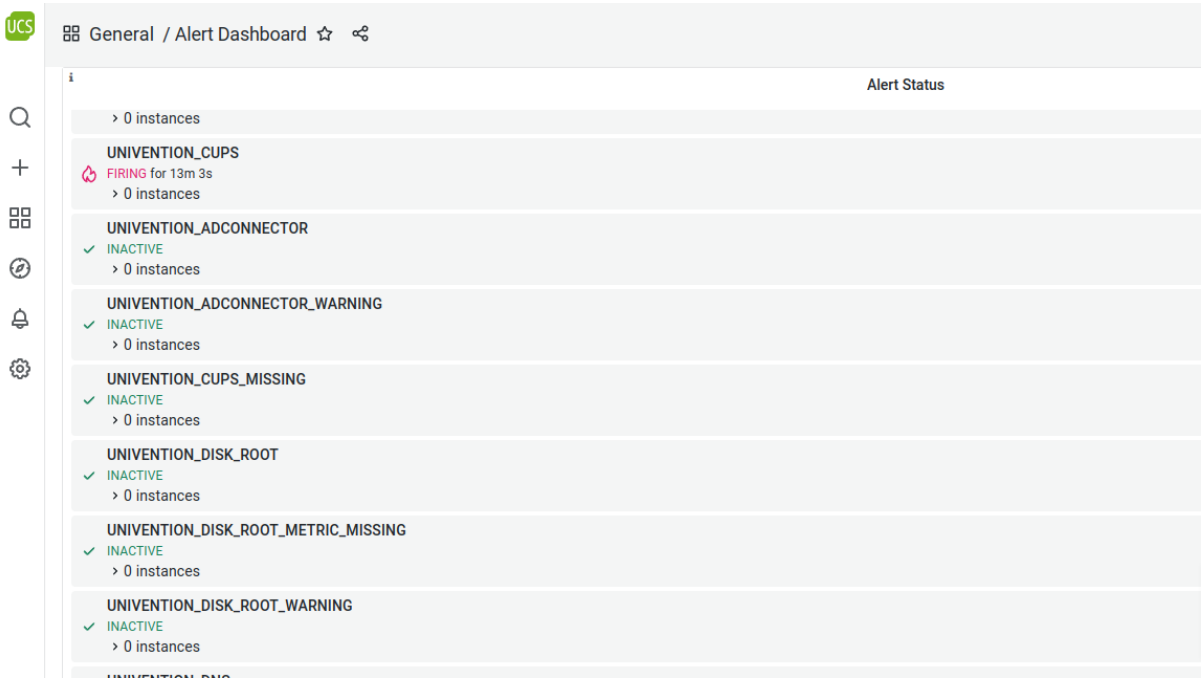


Abb. 15.3: *Alert Dashboard*

Standardmäßig konfiguriert die **UCS Dashboard** App das *Alert Dashboard*. Das *Alert Dashboard* zeigt detaillierte Informationen über den Status aller in UCS konfigurierten Alarme.

Eigene Dashboards

Administratoren können die drei enthaltenen Dashboards *Domain Dashboard*, *Server Dashboard* und *Alarm Dashboard* nicht ändern, da Univention Updates für sie bereitstellt.

Stattdessen können eigene Dashboards erstellt werden. Auf diesen Dashboards können dann entweder bereits vorhandene Elemente hinzugefügt werden oder auch neue Elemente erstellt werden. Dazu muss lediglich auf das Plus Zeichen am linken Rand geklickt werden. Anschließend existiert ein neues Dashboard, welches mit Elementen befüllt werden kann.

15.2 Monitoring

Neu in Version 5.0-2: UCS 5.0-2 unterstützt die Überwachung von Alarmen durch *Prometheus*-Metriken.

Mit *Prometheus*, *Prometheus Node Exporter*, und *Prometheus Alertmanager* können Administratoren die korrekte Funktion von komplexen IT-Strukturen aus Netzwerken, Rechnern und Diensten kontinuierlich und automatisch überprüfen.

Der Prometheus Node Exporter exportiert eine umfassende Sammlung von Metriken in die Prometheus Datenbank. Neben der Abfrage von Systemindikatoren wie CPU, Speichernutzung und freien Speicherplatz, testen sie die Verfügbarkeit und den Betrieb von verschiedenen Diensten wie SSH, SMTP und HTTP. Betriebstests führen im Allgemeinen Programmschritte wie die Zustellung einer Test-E-Mail oder die Auflösung eines DNS-Eintrags durch. Der Prometheus Node Exporter bietet UCS spezifische Alarme zusätzlich zu den bereits enthaltenen Startmetriken, zum Beispiel einen Alarm für die Listener/Notifier-Replikation.

Wenn sich der Betriebszustand ändert, informiert die Überwachung einen vorher festgelegten Ansprechpartner über die mögliche Störung. Zusätzlich zur reaktiven Benachrichtigung im Fehlerfall können Administratoren den aktuellen Status jederzeit kontinuierlich in der Web-Oberfläche *Grafana UCS Dashboard* , das die Statusinformationen kompakt anzeigt, überprüfen.

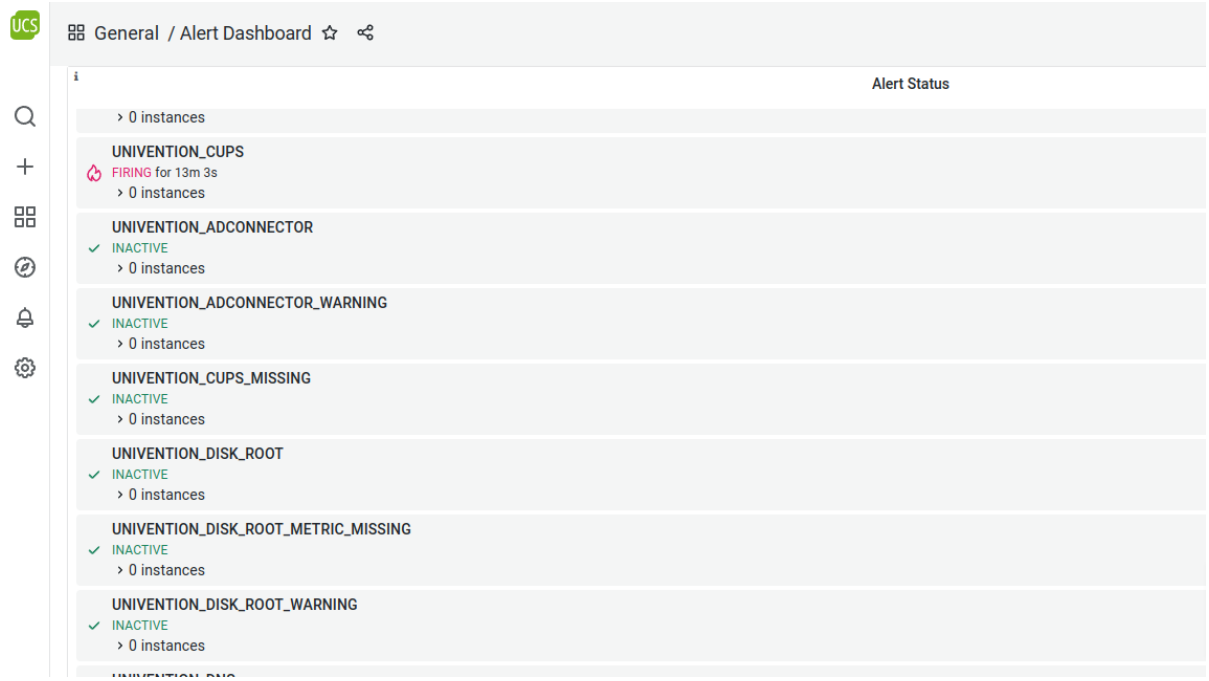


Abb. 15.4: Alert Dashboard

Siehe UCS Dashboard *Installation* (Seite 289) für eine Übersicht über alle beteiligten Komponenten.

Administratoren definieren die Alarmkonfiguration in Univention Management Console. Ein Listener Modul generiert automatisch die Konfigurationsdateien aus den Informationen im LDAP-Verzeichnis.

15.2.1 Installation

Zur Installation der UCS Dashboard Komponenten siehe *Installation* (Seite 289).

Zusätzlich zu den Komponenten des UCS Dashboards müssen Sie die App *Prometheus Alertmanager* und den *univention-monitoring-client* installieren.

Für jedes UCS-System, das der Administrator auf dem Dashboard anzeigen möchte, muss er die App *UCS Dashboard Client* installieren. Das Paket **univention-monitoring-client** hängt von *UCS Dashboard Client* ab und wird standardmäßig auf jedem UCS-System installiert, um die Alarmfunktionalität bereitzustellen.

Prometheus Alertmanager
: Die *Prometheus Alertmanager* App versendet Benachrichtigungen über ausgelöste Alarme, zum Beispiel per E-Mail. Der Alertmanager benötigt einige Einstellungen, um korrekt zu funktionieren.

Die Einstellungen umfassen die Empfänger der E-Mail-Benachrichtigungen. Außerdem benötigen die App-Einstellungen einen Wert für einen SMTP-Server, um E-Mail-Benachrichtigungen zu senden. Der Alertmanager unterstützt die SMTP-Authentifizierungsmethoden `PLAIN`, `LOGIN` und `CRAM-MD5` sowie die Kommunikation via TLS. Keine Authentifizierung wird verwendet, wenn Sie alle Felder der App-Einstellungen bezüglich Authentifizierung leer lassen.

univention-monitoring-client
: Das Paket **univention-monitoring-client** stellt Standard Alarm Plugins zur Überprüfung des Systemzustands bereit.

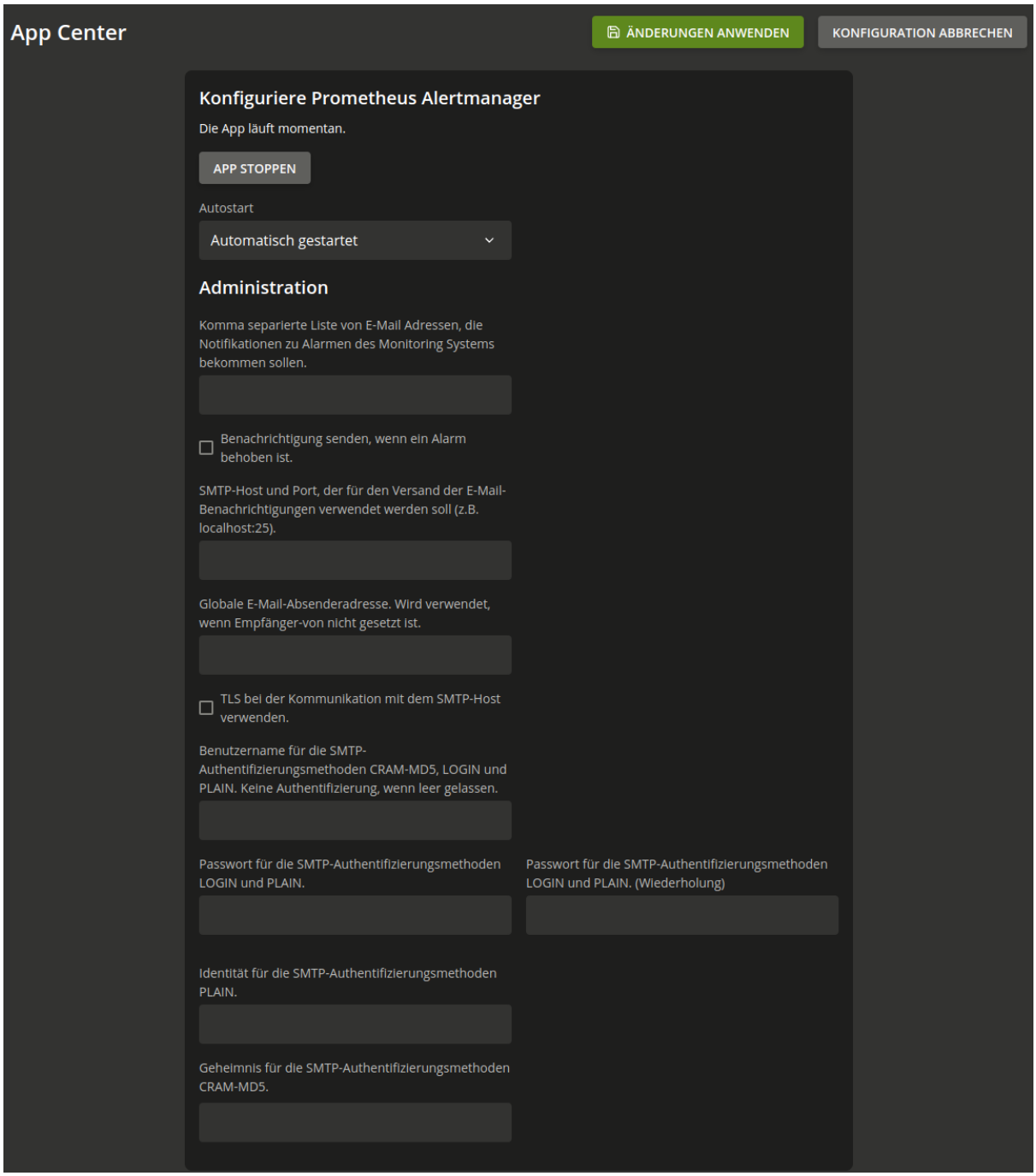
Administratoren können mit den folgenden Paketen Plugins installieren, die über die Standard-Plugins hinausgehen, die mit dem **univention-monitoring-client** Paket bereitgestellt werden.

- **univention-monitoring-raid**: Überwachung des Software-RAID-Status
- **univention-monitoring-smart**: Prüfung des S.M.A.R.T.-Status von Festplatten
- **univention-monitoring-opsi**: Prüfung der Software OPSI
- **univention-monitoring-cups**: Prüfung des Druckerdienstes CUPS
- **univention-monitoring-squid**: Prüfung des Squid proxy Servers
- **univention-monitoring-samba**: Prüfung des Samba 4 Dienstes
- **univention-monitoring-s4-connector**: Prüfung des S4-Connector
- **univention-monitoring-ad-connector**: Prüfung des AD Connectors

Einige Dienste richten ihr jeweiliges Paket zur Überwachung bereits bei der Installation ein. Wenn Administratoren zum Beispiel den **UCS AD Connector** einrichten, enthält es automatisch das Plugin für die Überwachung.

15.2.2 Vorkonfigurierte Überwachungstests

Die Installation richtet automatisch grundlegende Überwachungstests für UCS Systeme ein. Alle Alarme haben die Bezeichnung (*Label*) *severity* mit dem Wert `critical` oder `warning`.


App Center
ÄNDERUNGEN ANWENDEN
KONFIGURATION ABBRECHEN
Konfiguriere Prometheus Alertmanager
Die App läuft momentan.
APP STOPPEN
Autostart
Automatisch gestartet
Administration
Komma separierte Liste von E-Mail Adressen, die Notifikationen zu Alarmen des Monitoring Systems bekommen sollen.
Benachrichtigung senden, wenn ein Alarm behoben ist.
SMTP-Host und Port, der für den Versand der E-Mail-Benachrichtigungen verwendet werden soll (z.B. localhost:25).
Globale E-Mail-Absenderadresse. Wird verwendet, wenn Empfänger-von nicht gesetzt ist.
TLS bei der Kommunikation mit dem SMTP-Host verwenden.
Benutzername für die SMTP-Authentifizierungsmethoden CRAM-MD5, LOGIN und PLAIN. Keine Authentifizierung, wenn leer gelassen.
Passwort für die SMTP-Authentifizierungsmethoden LOGIN und PLAIN.
Passwort für die SMTP-Authentifizierungsmethoden LOGIN und PLAIN. (Wiederholung)
Identität für die SMTP-Authentifizierungsmethoden PLAIN.
Geheimnis für die SMTP-Authentifizierungsmethoden CRAM-MD5.

Tab. 15.1: Vorkonfigurierte Alarme

Alarm	Beschreibung
UNIVENTION_DISK_ROOT und UNIVENTION_DISK_ROOT_WARNING	Überwacht den Füllstand der /-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% oder 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit des öffentlichen DNS-Servers durch Abfrage des Rechnernamens www.univention.de. Wenn kein DNS-Forwarder für die UCS-Domäne definiert ist, schlägt diese Anfrage fehl. In diesem Fall kann www.univention.de durch den FQDN des Primary Directory Node ersetzt werden, zum Beispiel in der monitoring/dns/lookup-domain um die Funktion der Namensauflösung zu testen.
UNIVENTION_LDAP_AUTH	Überwacht den auf Directory Nodes laufenden LDAP-Server.
UNIVENTION_LOAD und UNIVENTION_LOAD_WARNING	Überwacht die Systemlast.
UNIVENTION_NTP und UNIVENTION_NTP_WARNING	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 oder 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	Testet, ob der SMTP-Server erreichbar ist. Der Alarm wird ausgelöst, wenn er nicht erreichbar ist.
UNIVENTION_SSL und UNIVENTION_SSL_WARNING	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Primary Directory Node und Backup Directory Nodes geeignet.
UNIVENTION_SWAP und UNIVENTION_SWAP_WARNING	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% oder 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION und UNIVENTION_REPLICATION_WARNING	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer failed.ldif-Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD und UNIVENTION_NSCD2	Testet die Verfügbarkeit des Name Server Cache Dienstes (NSCD). Läuft kein NSCD-Prozess wird ein *critical* Alarm ausgelöst, läuft mehr als ein Prozess, wird ein *warning* Alarm ausgelöst.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein *critical* Alarm ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den NetBIOS-Dienst zuständig ist. Läuft kein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_JOINSTATUS und UNIVENTION_JOINSTATUS_WARNING	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein *critical* Alarm ausgelöst, sind nicht-aufgerufene Join-Skripte vorhanden, wird ein *warning* Alarm ausgelöst.
UNIVENTION_KPASSWDD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Primary/Backup Directory Node). Läuft weniger oder mehr als ein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_PACKAGE_STATUS	Überwacht den Status der installierten Debian-Pakete. Wenn ein Paket den Status *half-installed* hat, wird ein Alarm ausgelöst.
UNIVENTION_SLAPD_MDB_MAXSIZE und UNIVENTION_SLAPD_MDB_MAXSIZE_WARNING	Überwacht den Anteil der freien Speicherseiten des *mdb* Backends von SLAPD für mehrere Verzeichnisse.
UNIVENTION_LISTENER_MDB_MAXSIZE und UNIVENTION_LISTENER_MDB_MAXSIZE_WARNING	Überwacht den Anteil der freien Speicherseiten des *mdb* Backends von SLAPD für mehrere Verzeichnisse.

Die folgenden Alarme sind nur verfügbar, sobald zusätzliche Pakete installiert wurden (siehe *Monitoring installation* (Seite 293))

Tab. 15.2: Zusätzliche Alarme

Alarm	Beschreibung
UNIVENTION_OPSI	Überwacht den OPSI-Daemon. Läuft kein OPSI-Prozess oder die OPSI-Weboberfläche ist nicht erreichbar, wird ein Alarm zurückgegeben.
UNIVENTION_SMART_SDA	Prüft den S.M.A.R.T.-Status der Festplatte `/dev/sda`. Für die Festplatten `sdb`, `sdc` und `sdd` existieren entsprechende Alarme.
UNIVENTION_RAID und UNIVENTION_RAID_WARNING	Prüft den Status des Software-RAIDs über `/proc/mdadm` und löst einen *critical* Alarm aus, sofern eine Festplatte des RAID-Verbunds ausgefallen ist, oder einen *warning* Alarm, wenn der Recovery-Vorgang läuft.
UNIVENTION_ADCONNECTOR und UNIVENTION_ADCONNECTOR_WARNING	Prüft den Status des Active Directory Connectors: • Läuft kein Connector-Prozess, wird ein Alarm zurückgegeben. • Existiert mehr als ein Prozess pro Connector-Instanz, wird ein *warning* Alarm ausgelöst. • Treten Rejects auf, wird ein *warning* Alarm ausgelöst. • Kann der AD-Server nicht erreicht werden, wird ein Alarm zurückgegeben. Das Plugin kann auch in Multi-Connector-Instanzen verwendet werden.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft der **cupsd**-Prozess nicht oder ist die Weboberfläche nicht erreichbar, wird ein *critical* Alarm ausgelöst.
UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird ein Alarm zurückgegeben.
UNIVENTION_RAID und UNIVENTION_RAID_WARNING	Überwacht den Status der vorhandenen RAID Geräte. Der *warning* Alarm wird im Falle folgender RAID Status ausgelöst: • `Rebuilding` • `Reconstruct` • `Replaced Drive` • `Expanding` • `Warning` • `Verify` Der *critical* Alarm wird für folgende RAID Status ausgelöst: • `Degraded` • `Dead` • `Failed` • `Error` • `Missing`
UNIVENTION_S4CONNECTOR und UNIVENTION_S4CONNECTOR_WARNING	Überwacht den Status des Samba 4 Servers. Ein *warning* Alarm wird ausgelöst, wenn der Samba 4 erreichbar ist, aber keine Ablehnungen (*rejects*) vorhanden sind. Ein *critical* Alarm wird ausgelöst, wenn der Server nicht erreichbar ist.
UNIVENTION_SAMBA_REPLICATION	Überwacht den Status der Samba-Replikation. Der Alarm wird ausgelöst, wenn ein Fehler der Replikation vorliegt.

15.2.3 Konfiguration

Univention Management Console bietet die folgenden Einstellungen:

- Administratoren müssen den Alarm konfigurieren (siehe *Monitoring installation* (Seite 293)) und festlegen, auf welchen Computern der Domäne ein Alarm aktiv sein soll (siehe *Zuweisung von Alarmen an Computer* (Seite 298)).
- Um die Kontaktperson zu konfigurieren, die der *Alertmanager* im Falle von Fehlern und Alarmen benachrichtigt, muss die entsprechende Einstellung in der **`Prometheus Alertmanager`** App gesetzt werden (siehe *Monitoring installation* (Seite 293)).
- Administratoren können Alarme für eine bestimmte Zeit stumm schalten. Siehe die Prometheus Alertmanager Dokumentation[68]. Benutzen Sie das *Prometheus Alertmanager* Webinterface für diese Einstellungen.

Die Grundeinstellungen definieren bereits eine Vielzahl von Tests für jeden Computer, z.B. eine Grundkonfiguration der Alarme, ohne dass weitere Anpassungen vorgenommen werden müssen.

Konfiguration der Alarme

Ein Alert definiert die Überwachung eines Dienstes oder eines Zustandes, zum Beispiel freier Festplattenspeicher. Administratoren können eine beliebige Anzahl von Computern einem solchen Alert-Objekt zuordnen.

Administratoren verwalten Alarme im UMC-Modul *Monitoring* mit dem Objekttyp *Alert*, siehe *Modul Rechnerverwaltung - Reiter Dienste* (Seite 152). Prometheus hat keine LDAP-Schnittstelle für die Überwachungskonfiguration. Stattdessen generiert ein Listener-Modul die Konfigurationsdateien, wenn Administratoren Alarme hinzufügen, bearbeiten oder entfernen.

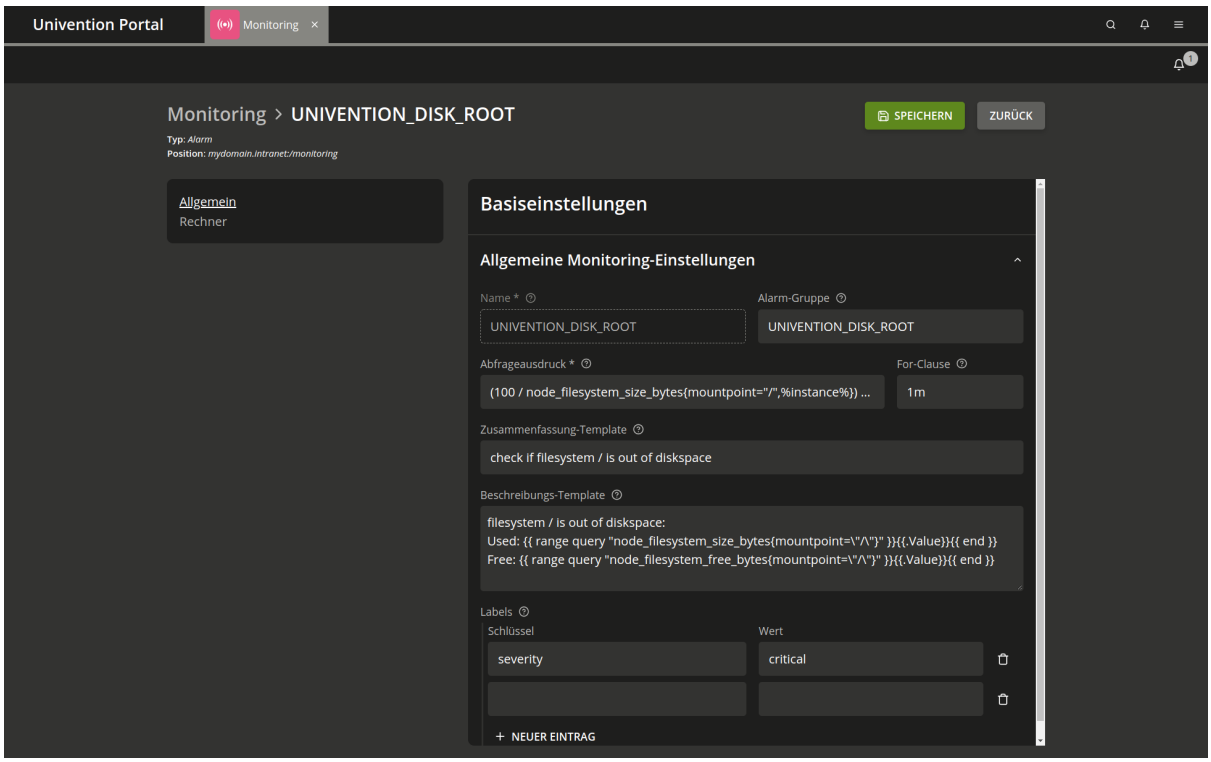


Abb. 15.5: Konfiguration eines Alarms

[68] https://prometheus.io/docs/alerting/latest/alertmanager/#silences

Tab. 15.3: Reiter *Allgemein*

Attribut	Beschreibung
`Name`	Eine eindeutige Bezeichnung für den Alarm.
`Alarm-Gruppe`	Legt die Gruppe fest, die den Alarm enthält. Mehrere Alarme können derselben Gruppe angehören.
`Abfrageausdruck`	Prometheus Abfrage, die den Alarm auslöst. Der Alarm wird ausgelöst, wenn die angegebene Abfrage einen nicht leeren Vektor zurück gibt. Für Details zur Syntax, siehe die Prometheus documentation[69].
`For-Clause`	Definiert die Zeit, in der das Ergebnis des Abfrageausdrucks nicht leer sein muss, bis der Alarm ausgelöst wird.
`Vorlage für Zusammenfassung`	Der Titel des Alarms, der im Dashboard und in den E-Mail-Benachrichtigungen für Alarme angezeigt wird.
`Vorlage für Beschreibung`	Die Beschreibung des Alarms, die im Dashboard und in den E-Mail-Benachrichtigungen für Alarme angezeigt wird.
`Labels`	Prometheus fügt den Alarmen Bezeichnungen (*Labels*) hinzu. Bezeichnungen helfen bei der Abfrage von Alarmen. Zum Beispiel: *severity* mit dem Wert `critical` oder `warning`.
`Vorlagenwerte`	Abfrageausdrücke, Beschreibungen und Zusammenfassungen können variable Werte verwenden. Zum Beispiel: Referenziere `max` durch `%max%`.

Tab. 15.4: Reiter *Rechner*

Attribut	Beschreibung
`Zugeordnete Rechner`	*Prometheus* führt die Abfrage auf den hier referenzierten Rechnern aus. Das Listener Modul führt die Tests für den Alert aus. Es ersetzt den Begriff `%instance%` im Abfrageausdruck durch einen regulären Ausdruck, der mit den zugewiesenen Rechnern übereinstimmt.

Zuweisung von Alarmen an Computer

Prometheus kann alle Computer überwachen, die mit Univention Management Console verwaltet werden.

Navigieren Sie in Univention Management Console zu *Computers* und wählen Sie den Computer aus, auf dem Sie Alarme aktivieren möchten. Wählen und fügen Sie die gewünschten Alarme im Reiter *Erweiterte Einstellungen* unter *Warnmeldungen* aus und speichern Sie Ihre Änderungen.

Tab. 15.5: Reiter *Erweiterte Einstellungen*

Attribut	Beschreibung
`zugewiesene Warnmeldungen`	Listet alle zugewiesenen Alarme für den aktuellen Computer auf. Fügen Sie hier Alarme hinzu oder entfernen Sie sie.

[69] https://prometheus.io/docs/prometheus/latest/querying/basics/

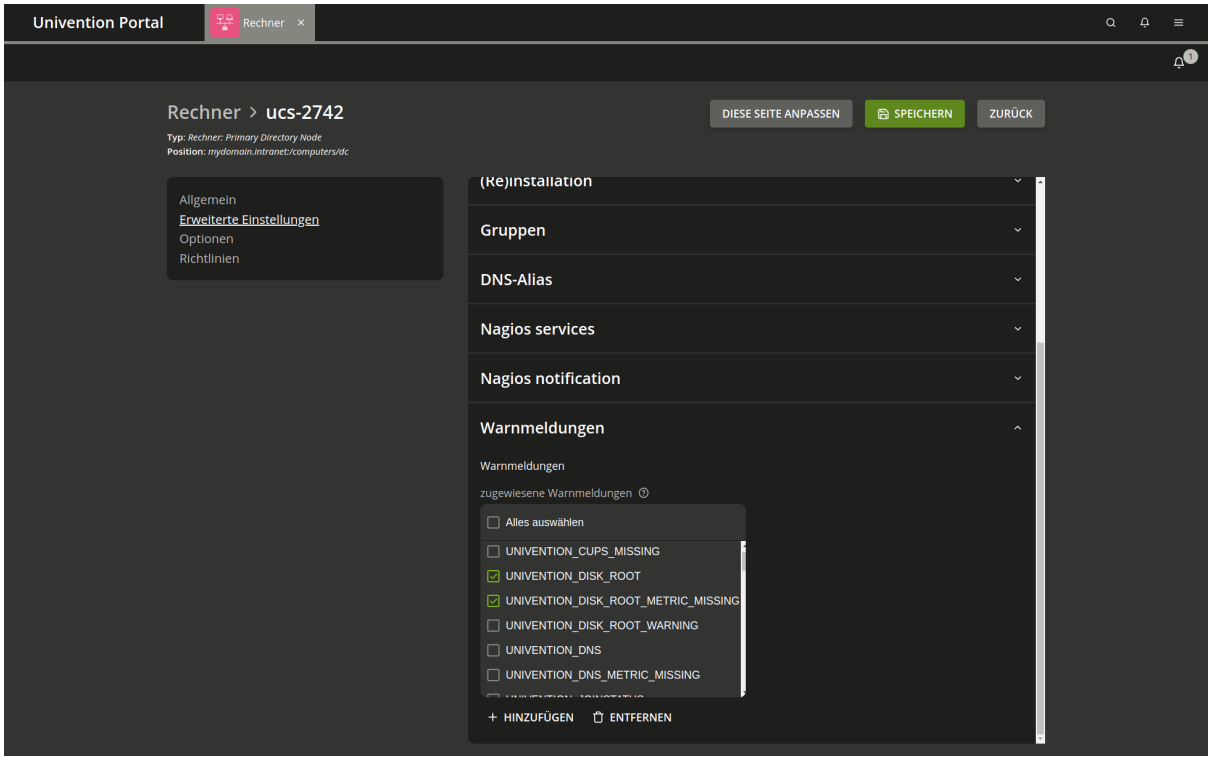


Abb. 15.6: Zuweisung eines Alarms an einen Computer

Neue Alarme erstellen

In diesem Abschnitt wird beschrieben, wie Sie ein benutzerdefiniertes Skript hinzufügen, um neue Metriken zu sammeln und Alarme zu erstellen.

Als Administrator können Sie die vorkonfigurierten Alarme, die mit UCS geliefert werden, durch zusätzliche Alarme ergänzen. Ein Alarmprüfung Skript exportiert Metriken über den Rechner, auf dem es läuft, an *Prometheus*. Eine *PromQL*-Abfrage auf Metriken definiert einen Alarm in *Prometheus*. Für weitere Informationen darüber, wie man eigene benutzerdefinierte Checks schreibt, siehe Querying basis[70].

Kopieren Sie das benutzerdefinierte Alarmprüfung Skript in das Verzeichnis `/usr/share/univention-monitoring-client/scripts/` auf dem UCS-System, das die benutzerdefinierten Metriken exportieren soll. Ändern Sie den Dateimodus auf *ausführbar* mit **`chmod a+x PLUGIN`**.

Alle von UCS gelieferten Alert Checks verwenden Python. Benutzerdefinierte Prüfungen können Perl, Python oder Shell verwenden und benötigen keine externen Bibliotheken oder Programme. Alle UCS-Systeme stellen immer die benötigten Interpreter zur Verfügung.

Verwendet die benutzerdefinierte Alarmprüfung dagegen externe Programme oder Bibliotheken, müssen Sie diese auf allen UCS-Systemen installieren, die die benutzerdefinierte Prüfung verwenden sollen.

Das Skript für die Alarmprüfung exportiert eine oder mehrere Metriken, indem es sie in eine `.prom` Datei im `/var/lib/prometheus/node-exporter/` Verzeichnis schreiben. *Prometheus* importiert diese Datei.

Sie müssen den benutzerdefinierten Alarm in Univention Management Console konfigurieren, siehe *Konfiguration der Alarme* (Seite 297). Sie müssen einen Prometheus Ausdruck für die Metrik des Skripts in das Feld *Query expression* eingeben. Um den benutzerdefinierten Alert zu UCS-Systemen zuzuordnen, siehe *Zuweisung von Alarmen an Computer* (Seite 298).

Siehe auch:

[70] https://prometheus.io/docs/prometheus/latest/querying/basics/

Prometheus Namenskonventionen
Metric and label naming[71]

Text-basiertes Format einer `.prom`-Datei
Exposition formats[72]

15.3 Nagios

In UCS 5.0 ist die Serverkomponente von Nagios nicht mehr unterstützt. Die Systeme können aber als Nagios Client dienen, um sie z.B. von einem UCS 4.4 Nagios Server überwachen zu lassen, wie im UCS 4.4 Handbuch beschreiben.

15.3.1 Installation

Neben den Standard-Plugins, die mit der Installation des Pakets **`univention-nagios-client`** mitgebracht werden, können zusätzliche Plugins über folgende Pakete nachinstalliert werden:

- **`univention-nagios-raid`** Überwachung des Software-RAID-Status
- **`univention-nagios-smart`** Prüfung des S.M.A.R.T.-Status von Festplatten
- **`univention-nagios-opsi`** Prüfung der Softwareverteilung OPSI
- **`univention-nagios-ad-connector`** Prüfung des AD-Connectors

Einige der Pakete werden bei der Installation der entsprechenden Dienste automatisch mit eingerichtet. Wird beispielsweise der UCS AD Connector eingerichtet, bringt dieser das Überwachungsplugin **`univention-nagios-ad-connector`** mit.

15.3.2 Vorkonfigurierte Nagios-Prüfungen

Während der Installation werden automatisch grundlegende Nagios-Prüfungen für die UCS-Systeme der Domäne eingerichtet.

[71] https://prometheus.io/docs/practices/naming/
[72] https://prometheus.io/docs/instrumenting/exposition_formats/

Tab. 15.6: Vorkonfigurierte Nagios-Prüfungen

Nagios-Dienst	Beschreibung
UNIVENTION_PING	Testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando **ping**. In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50 ms oder 100 ms überschreitet oder Paketverluste von 20% oder 40% auftreten.
UNIVENTION_DISK_ROOT	Überwacht den Füllstand der /-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% oder 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit der öffentlichen DNS-Server durch die Abfrage des Rechnernamens www.univention.de. Ist für die UCS-Domäne kein DNS-Forwarder definiert, schlägt diese Abfrage fehl. In diesem Fall kann www.univention.de z.B. gegen den FQDN des Primary Directory Node ersetzt werden, um die Funktion der Namensauflösung zu testen.
UNIVENTION_LDAP	Überwacht den auf Directory Nodes laufenden LDAP-Server.
UNIVENTION_LOAD	Überwacht die Systemlast.
UNIVENTION_NTP	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 oder 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	Testet den Mailserver.
UNIVENTION_SSL	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Primary Directory Node und Backup Directory Nodes geeignet.
UNIVENTION_SWAP	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% oder 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer failed.ldif-Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD	Testet die Verfügbarkeit des Name Server Cache Dienstes (NSCD). Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess, wird ein WARNING-Event ausgelöst.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den NetBIOS-Dienst zuständig ist. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_JOINSTATUS	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein CRITICAL-Event ausgelöst, sind nicht-aufgerufene Join-Skripte vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWDD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Primary/Backup Directory Node). Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft **cupsd**-Prozess oder ist die Weboberfläche auf Port 631 nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.

Die folgenden Nagios-Dienste sind nur auf dem jeweiligen Nagios Client verfügbar, sobald zusätzliche Pakete installiert wurden (siehe *Installation* (Seite 300)):

Tab. 15.7: Zusätzliche Nagios Checks

Nagios-Dienst	Beschreibung
UNIVENTION_OPSI	Überwacht den OPSI-Daemon. Läuft kein OPSI-Prozess oder die OPSI-Weboberfläche ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SMART_SDA	Prüft den S.M.A.R.T.-Status der Festplatte /dev/sda. Für die Festplatten sdb, sdc und sdd existieren entsprechende Nagios-Dienste.
UNIVENTION_RAID	Prüft den Status des Software-RAIDs über /proc/mdadm und gibt einen CRITICAL Alarm zurück, sofern eine Festplatte des RAID-Verbunds ausgefallen ist, oder einen WARNING Alarm zurück, wenn der Recovery-Vorgang läuft.
UNIVENTION_ADCONNECTOR	Prüft den Status des Active Directory Connectors: • Läuft kein Connector-Prozess, wird der Status CRITICAL zurückgegeben. • Existiert mehr als ein Prozess pro Connector-Instanz gibt es eine WARNING. • Treten Rejects auf, gibt es eine WARNING. • Kann der AD-Server nicht erreicht werden, tritt ein CRITICAL-Zustand ein. Das Plugin kann auch in Multi-Connector-Instanzen verwendet werden. Dabei muss der Name der Instanz als Parameter übergeben werden.

KAPITEL 16

Anhang

16.1 Univention Configuration Registry Variablen

Dieser Anhang listet Univention Configuration Registry Variablen auf, die im Handbuch erwähnt werden.

auth/faillog

Konfiguriert das automatische Sperren von Benutzern nach fehlgeschlagenen Anmeldungen im PAM Stack. Zum Aktivieren, setze den Wert auf `yes`. Für mehr Informationen, siehe *PAM-Stack* (Seite 133).

auth/faillog/limit

Konfiguriert die Obergrenze an fehlerhaften Anmeldeversuchen für eine Benutzerkontosperre. Für mehr Informationen, siehe *PAM-Stack* (Seite 133).

auth/faillog/lock_global

Konfiguriert auf Primary Directory Node und Backup Directory Node eine globale Sperre nach fehlerhaften Anmeldeversuchen im LDAP-Verzeichnis. Für mehr Informationen, siehe *PAM-Stack* (Seite 133).

auth/faillog/root

Um das Benutzerkonto `root` der Sperrung des PAM-Stack-Kontos zu unterwerfen, setzen Sie den Wert auf `yes`. Die Voreinstellung ist `no`. Für weitere Informationen, siehe *PAM-Stack* (Seite 133).

auth/faillog/unlock_time

Legen Sie ein Zeitintervall fest, in dem eine Kontosperre aufgehoben wird. Der Wert wird in Sekunden angegeben. Der Wert `0` setzt die Sperre sofort zurück. Für weitere Informationen, siehe *PAM-Stack* (Seite 133).

auth/sshd/user/root

Um die SSH-Anmeldung für den Benutzer `root` komplett zu verbieten, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 174).

backup/clean/max_age

Legt fest, wie lange ein UCS-System alte Sicherungsdateien der LDAP-Daten aufbewahrt. Erlaubte Werte sind ganzzahlige Zahlen und definieren Tage. Das System löscht keine Sicherungsdateien, wenn die Variable nicht gesetzt ist. Siehe *Tägliche Sicherung der LDAP-Daten* (Seite 41).

connector/ad/ldap/binddn

Konfiguriert den LDAP-DN eines privilegierten Replikationsbenutzers. Für weitere Informationen, siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 188) und *Änderung des AD-Zugriffspassworts* (Seite 195).

connector/ad/ldap/bindpw

Legt das Passwort eines privilegierten Replikationsbenutzers fest. Für weitere Informationen, siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 188) und *Änderung des AD-Zugriffspassworts* (Seite 195).

connector/ad/ldap/ssl

Um die verschlüsselte Kommunikation zwischen dem UCS System und Active Directory zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Import des SSL-Zertifikats des Active Directory* (Seite 194).

connector/ad/mapping/group/language

Konfiguriert die Zuordnung für die Umwandlung von Gruppennamen in anglophonen AD Domänen. Für weitere Informationen, siehe *Gruppen* (Seite 202).

connector/ad/poll/sleep

Konfiguriert das Intervall für die Abfrage nach Änderungen in der AD-Domäne. Die Voreinstellung ist `5` Sekunden. Für weitere Informationen, siehe *Einrichtung des UCS AD-Connectors* (Seite 191).

connector/ad/retryrejected

Konfiguriert die Anzahl der Zyklen, die der UCS AD Connector versucht, ein Objekt aus der AD-Domäne zu synchronisieren, wenn es nicht synchronisiert werden kann. Der Standardwert ist `10` Zyklen. Für weitere Informationen, siehe *Einrichtung des UCS AD-Connectors* (Seite 191).

cups/cups-pdf/anonymous

Legt das Zielverzeichnis für den *Generic CUPS-PDF Printer* für anonyme Druckaufträge fest. Standardmäßig ist dies der Wert `/var/spool/cups- pdf/`. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 265).

cups/cups-pdf/cleanup/enabled

Um veraltete Druckaufträge des *Generic CUPS-PDF Printer* zu bereinigen, setzen Sie den Wert auf `true`. Für die Speicherzeit, siehe *`cups/cups-pdf/cleanup/keep`* (Seite 304). Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 265).

cups/cups-pdf/cleanup/keep

Legt die Speicherzeit in Tagen für PDF-Dateien aus dem *Generic CUPS-PDF Printer* fest. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 265).

cups/cups-pdf/directory

Legt das Zielverzeichnis für den *Generic CUPS-PDF Printer* fest. Standardmäßig ist dies der Wert `/var/spool/cups-pdf/%U` und verwendet für jeden Benutzer ein anderes Verzeichnis. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 265).

cups/errorpolicy

Um fehlgeschlagene Druckaufträge automatisch alle 30 Sekunden zu wiederholen, setzen Sie den Wert auf `retry-job`. Für weitere Informationen, siehe *Einstellung lokaler Konfigurationseigenschaften eines Druckservers* (Seite 260).

cups/include/local

Um die Konfiguration aus `/etc/cups/cupsd.local.conf` einzubeziehen, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Einstellung lokaler Konfigurationseigenschaften eines Druckservers* (Seite 260).

cups/server

Definiert den Druckserver, der von einem UCS-System verwendet werden soll. Für weitere Informationen, siehe *Konfiguration des verwendeten Druckservers* (Seite 170).

directory/manager/blocklist/cleanup/cron

Diese Variable bestimmt, wie oft UDM nach abgelaufenen Blocklisteneinträge sucht und diese entfernt. Der Wert folgt der *cron Syntax* (Seite 172) für die Zeitdefinition. Der Standardwert ist auf täglich um 8:00 Uhr morgens gesetzt. Weitere Informationen finden Sie unter *Abgelaufene Blocklisteneinträge* (Seite 138).

directory/manager/blocklist/enabled

Aktiviert die Verwaltung von Blocklisteneinträgen in UDM. Der Standardwert ist `false`. Für Informationen über die Aktivierung, siehe *Aktivieren von Blocklisten* (Seite 136).

directory/manager/templates/alphanum/whitelist

Definieren Sie eine Erlaubnisliste von Zeichen, die nicht durch die Option `:alphanum` für die Wertedefinition in Benutzervorlagen entfernt werden. Für weitere Informationen, siehe *Benutzervorlagen* (Seite 134).

directory/manager/user_group/uniqueness

Steuert, ob UCS Benutzer mit demselben Benutzernamen wie bestehende Gruppen verhindert. Um die Prüfung auf Eindeutigkeit zu deaktivieren, setzen Sie den Wert auf `false`. Für weitere Informationen, siehe Tab. 6.1.

directory/manager/web/modules/computers/computer/wizard/disabled

Um den vereinfachten Assistenten für die Computerverwaltung zu deaktivieren, setzen Sie diese Variable auf `true`. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 147).

directory/manager/web/modules/groups/group/checks/circular_dependency

Steuert die Prüfung auf zirkuläre Abhängigkeiten bei verschachtelten Gruppen. Um sie zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Verschachtelte Gruppen mit Gruppen in Gruppen* (Seite 143).

directory/manager/web/modules/users/user/wizard/disabled

Deaktiviert den vereinfachten Assistenten zum Anlegen von Benutzern, wenn der Wert auf `true` gesetzt ist. In der Standardeinstellung ist der Assistent aktiviert. Für weitere Informationen, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 110).

directory/reports/logo

Definiert den Pfad und den Namen einer Bilddatei zur Verwendung als Logo in einer Univention Directory Report PDF-Datei. Für weitere Informationen, siehe *Anpassung/Erweiterung von Univention Directory Reports* (Seite 93).

dns/allow/transfer

Um den DNS-Zonentransfer bei Verwendung des OpenLDAP-Backends zu deaktivieren, setzen Sie den Wert auf `none`. Für weitere Informationen, siehe *Konfiguration von Zonentransfers* (Seite 222).

dns/backend

Konfiguriert das DNS-Backend. Für weitere Informationen, siehe *Konfiguration des Daten-Backends des Nameservers* (Seite 222).

dns/debug/level

Konfiguriert den Debug-Level für BIND. Für weitere Informationen, siehe *Konfiguration der Debug-Ausgaben von BIND* (Seite 222).

dns/dlz/debug/level

Konfiguriert den Debug-Level für das Samba DNS Backend. Für weitere Informationen, siehe *Konfiguration der Debug-Ausgaben von BIND* (Seite 222).

dns/forwarder1

Definiert den ersten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

dns/forwarder2

Definiert den zweiten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

dns/forwarder3

Definiert den dritten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

fetchmail/autostart

Steuert den automatischen Start von Fetchmail. Um Fetchmail zu deaktivieren, setzen Sie den Wert auf `false`. Für weitere Informationen, siehe *Integration von Fetchmail zum Abrufen von Mail von externen Postfächern* (Seite 279).

freeradius/auth/helper/ntlm/debug

Konfiguriert den Debug-Level oder die Ausführlichkeit für die Protokollierung von FreeRADIUS-Meldungen. Für weitere Informationen, siehe *Fehlersuche* (Seite 246).

freeradius/conf/allow-mac-address-authentication

Konfiguriert, ob Radius die MAC-Adresse als Benutzernamen und Passwort für die 802.1X-Authentifizierung zulässt. Der Standardwert ist `false`. Für weitere Informationen, siehe *MAC Authentication Bypass für Computerobjekte* (Seite 242).

freeradius/conf/mac-addr-regexp

Konfiguriert den regulären Ausdruck für die MAC-Adresse für den Radius Server. Der reguläre Ausdruck muss sechs Gruppen enthalten, wobei jede Gruppe ein Byte der MAC-Adresse darstellt.

Der Standardwert ist der reguläre Ausdruck: `([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})`

Neu in Version 5.0-6-erratum-…: Mit UCS 5.0 erratum 1011[73] kann der Radius-Server mit verschiedenen Formaten der MAC-Adressen für den Benutzernamen bei Verwendung von MAB umgehen.

Für weitere Informationen und Effekte, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 280).

freeradius/vlan-id

Konfiguriert den Ersatzwert für die VLAN-ID für Benutzer, die nicht Mitglied einer Gruppe mit einer VLAN-ID sind. Für weitere Informationen, siehe *VLAN IDs* (Seite 245).

gateway

Konfiguriert das IPv4-Netzwerk-Gateway. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 156).

google-apps/attributes/anonymize

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das Google Apps for Work Connector synchronisiert, aber mit zufälligen Daten füllt. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Für weitere Informationen, siehe *Konfiguration* (Seite 217).

google-apps/attributes/mapping/.*

Definiert eine Zuordnung von UCS LDAP-Attributen eines Benutzerkontos für die Synchronisation zu Google Apps Attributen. Die Standardeinstellungen reichen in der Regel für die meisten Umgebungsanforderungen aus. Für weitere Informationen, siehe *Konfiguration* (Seite 217).

google-apps/attributes/never

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Google Apps for Work Connector nie synchronisiert, auch wenn sie in *google-apps/attributes/mapping/.** (Seite 306) oder *google-apps/attributes/anonymize* (Seite 306) erwähnt werden. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Konfiguration* (Seite 217).

google-apps/debug/werror

Konfigurieren Sie zusätzliche Debugausgaben für Google Apps for Work. Für weitere Informationen, siehe *Fehlersuche* (Seite 217).

google-apps/groups/sync

Ermöglicht die Synchronisation von Gruppen der Google Apps for Work Benutzergruppen mit dem Wert `yes`. Für weitere Informationen, siehe *Konfiguration* (Seite 217).

[73] https://errata.software-univention.de/#/?erratum=5.0x1011

groups/default/domainadmins

Konfiguriert den Standardgruppennamen für die Domänenadministratorgruppe. Der Wert kann während einer AD-Übernahme geändert werden. Für weitere Informationen, siehe *Domänenmigration* (Seite 204).

grub/append

Definiert Linux-Kernel-Boot-Optionen, die der GRUB-Bootloader an den Linux-Kernel zum Systemstart weitergibt. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 154).

grub/bootsplash

Um den Splash-Screen beim Systemstart zu deaktivieren, setzen Sie den Wert auf `nosplash`. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 154).

grub/gfxmode

Legt die Bildschirmgröße und Farbtiefe für das GRUB-Bootmenü fest. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 154).

grub/timeout

Legt die Wartezeit in Sekunden im GRUB-Bootmenü fest. Während dieser Wartezeit können alternative Bootmenüeinträge ausgewählt werden. Der Standardwert ist `5` Sekunden. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 154).

grub/xenhopt

Legt Optionen fest, die an den Xen-Hypervisor übergeben werden. Weitere Informationen finden Sie unter *GRUB Boot-Manager* (Seite 154).

interfaces/ethX/address

Legt die Netzwerk-IPv4-Adresse für die Schnittstelle `eth`*X* fest. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 156).

interfaces/ethX/netmask

Definiert die Netzwerkmaske für die Schnittstelle `eth`*X*. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 156).

interfaces/ethX/type

Legt den Netzwerkschnittstellentyp für die Schnittstelle `eth`*X* fest. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 156).

interfaces/ethX_Y/setting

Definiert eine zusätzliche virtuelle Schnittstelle. Ersetzen Sie *X* und *Y* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 156).

interfaces/ethX/ipv6/address

Legt die Netzwerk-IPv6-Adresse für die Schnittstelle `eth`*X* fest. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 156).

interfaces/ethX/ipv6/prefix

Legt das Netzwerk-IPv6-Präfix für die Schnittstelle `eth`*X* fest. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 156).

interfaces/ethX/ipv6/acceptRA

Aktiviert die zustandslose Adressautokonfiguration (SLAAC) für die Schnittstelle `eth`*X*. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 156).

ipv6/gateway

Konfiguriert das IPv4-Netzwerk-Gateway. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 156).

kerberos/adminserver

Definiert das System, das den Kerberos-Adminserver bereitstellt. Siehe *Kerberos Adminserver* (Seite 45).

kerberos/kdc

Enthält den Verweis auf den KDC. Normalerweise wählt ein UCS-System den zu verwendende KDC aus einem DNS-Diensteintrag aus. Mit dieser Variable können Administratoren einen alternativen KDC konfigurieren.

kerberos/realm

Enthält den Namen des Kerberos-Realms. Siehe *Kerberos* (Seite 45).

kernel/blacklist

Definiert zusätzliche Linux-Kernelmodule, die während des Systemstarts geladen werden müssen. Einzelne Elemente müssen durch ein Semikolon (`;`) getrennt werden. Für weitere Informationen, siehe *Treiber-Management / Kernel-Module* (Seite 153).

kernel/modules

Definiert Linux-Kernel-Module, die beim Systemstart nicht geladen werden dürfen. Einzelne Einträge müssen mit einem Semikolon (`;`) getrennt werden. Für weitere Informationen, siehe *Treiber-Management / Kernel-Module* (Seite 153).

ldap/database/internal/acl/blocklists/groups/read

Liste der DNs von Gruppen, die Lesezugriff auf alle Objekte unter dem Container `cn=blocklists` in der internen Datenbank haben. Für weitere Informationen, siehe *LDAP ACLs für Blocklisten* (Seite 138).

ldap/database/internal/acl/blocklists/groups/write

Liste der DNs von Gruppen, die Schreibzugriff auf alle Objekte unter dem Container `cn=blocklists` in der internen Datenbank haben. Für weitere Informationen, siehe *LDAP ACLs für Blocklisten* (Seite 138).

ldap/acl/read/anonymous

Steuert, ob der LDAP-Server anonymen Zugriff auf das LDAP-Verzeichnis zulässt. In der Standardkonfiguration lässt der LDAP-Server keinen anonymen Zugriff auf das LDAP-Verzeichnis zu.

ldap/acl/read/ips

Eine Liste von IP-Adressen, für die der LDAP-Server anonymen Zugriff erlaubt. Siehe *Zugriffskontrolle auf das LDAP-Verzeichnis* (Seite 39).

ldap/acl/nestedgroups

Steuert, ob verschachtelte Gruppen erlaubt sind. Standardmäßig sind verschachtelte Gruppen aktiviert. Siehe *Zugriffskontrolle auf das LDAP-Verzeichnis* (Seite 39).

ldap/acl/user/passwordreset/accesslist/groups/dn

Verwenden Sie eine andere Gruppe als die Standardgruppe `User Password Admins`, um Benutzerpasswörter zurückzusetzen. Der Wert ist ein Distinguished Name (DN) für eine Benutzergruppe. Siehe *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 40).

ldap/acl/user/passwordreset/attributes

Wenn Benutzer, die die Passwörter anderer Benutzer ändern dürfen, Zugriff auf zusätzliche LDAP-Attribute benötigen, die für die Passwortänderung erforderlich sind, konfigurieren Sie diese in dieser Variablen. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 40).

ldap/acl/user/passwordreset/protected/uid

Konfiguriert Benutzer mit ihrer Benutzerkennung, um sie vom Zurücksetzen von Benutzerpasswörtern durch Administratoren, die Benutzerpasswörter ändern dürfen, auszuschließen. Trennen Sie mehrere Werte mit einem Komma. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 40).

ldap/acl/user/passwordreset/protected/gid

Konfiguriert Gruppen mit ihrer Gruppenkennung, um sie vom Zurücksetzen von Benutzerpasswörtern durch Administratoren, die Benutzerpasswörter ändern dürfen, auszuschließen. Trennen Sie mehrere Werte mit einem Komma. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 40).

ldap/idletimeout

Konfiguriert eine Zeitspanne in Sekunden, nach der die LDAP-Verbindung auf der Serverseite unterbrochen wird. Siehe *Timeout für inaktive LDAP-Verbindungen* (Seite 39).

ldap/logging/exclude1

Einzelne Bereiche des Verzeichnisdienstes von der Protokollierung ausschließen. Siehe *Revisionssichere LDAP-Protokollierung* (Seite 37).

ldap/logging/excludeN

Siehe `ldap/logging/exclude1` (Seite 309).

ldap/logging/id-prefix

Fügt die Transaktions-ID eines Eintrags in das Verzeichnisprotokoll ein. Mögliche Werte sind der Standardwert `yes` und `no`. Siehe *Revisionssichere LDAP-Protokollierung* (Seite 37).

ldap/master

Enthält den FQDN des Primary Directory Node in der Domäne.

ldap/overlay/lastbind

Um das `lastbind`-Overlay-Modul für den LDAP-Server zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos* (Seite 135).

ldap/overlay/lastbind/precision

Legt die Zeit in Sekunden fest, die vergehen muss, bevor der `authTimestamp` durch das `lastbind`-Overlay wieder aktualisiert wird. Für weitere Informationen, siehe *Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos* (Seite 135).

ldap/overlay/memberof/memberof

Konfiguriert das Attribut bei Benutzerobjekten, das die Gruppenzugehörigkeit anzeigt. Standardwert ist `memberOf`. Für weitere Informationen, siehe *Overlay-Modul zur Anzeige der Gruppeninformationen an Benutzerobjekten* (Seite 145).

ldap/policy/cron

Zeitintervall für das Schreiben profilbasierter UCR-Variablen in ein UCS-System. Der Standardwert ist eine Stunde. Für weitere Informationen, siehe *Richtlinienbasierte Konfiguration von UCR-Variablen* (Seite 164).

ldap/ppolicy

Um die automatische Kontosperrung zu aktivieren, setzen Sie den Wert auf `yes`. Setzen Sie auch `ldap/ppolicy/enabled` (Seite 309). Für weitere Informationen, siehe *OpenLDAP* (Seite 133).

ldap/ppolicy/enabled

Um die automatische Kontosperrung zu aktivieren, setzen Sie den Wert auf `yes`. Setzen Sie auch `ldap/ppolicy` (Seite 309). Für weitere Informationen, siehe *OpenLDAP* (Seite 133).

ldap/pw-bcrypt

Aktiviert **bcrypt** als Passworthash-Methode, wenn auf `true` gesetzt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 46).

ldap/server/addition

Zusätzlicher LDAP-Server, den ein UCS-System nach Informationen im Verzeichnisdienst abfragen kann.

ldap/server/name

Der LDAP-Server, den das System nach Informationen im Verzeichnisdienst abfragt.

listener/debug/level

Legt die Detailebene für Protokollmeldungen des Listeners in `/var/log/univention/listener.log` fest. Die möglichen Werte reichen von 0 (nur Fehlermeldungen) bis 4 (alle Statusmeldungen). Nach einer Änderung des Debug-Levels muss der Univention Directory Listener neu gestartet werden.

listener/shares/rename

Inhalte bestehender Freigabeverzeichnisse werden verschoben, wenn der Pfad zu einer Freigabe geändert wird und der Wert auf `yes` gesetzt wird. Für weitere Informationen, siehe Tab. 12.1 in *Freigaben UMC Modul - Reiter Allgemein* (Seite 249).

local/repository

Aktiviert und deaktiviert das lokale Repository. Für weitere Informationen, siehe *Einrichtung und Aktualisierung eines lokalen Repositorys* (Seite 103).

logrotate/compress

Steuert, ob rotierte Protokolldateien mit **gzip** komprimiert werden. Für weitere Informationen, siehe *Logdateien* (Seite 170).

log/rotate/weeks

Konfiguriert das Rotationsintervall der Protokolldateien auf einem UCS-System in Wochen. Der Standardwert ist `12` Wochen. Für weitere Informationen, siehe *Logdateien* (Seite 170).

logrotate/rotates

Konfiguriert die Rotation der Protokolldateien entsprechend der Dateigröße, zum Beispiel `size 50M`. Für weitere Informationen, siehe *Logdateien* (Seite 170).

machine/password/length

Definieren Sie die Länge des Computer-Passworts, auch *machine secret* genannt. Der Standardwert ist `20`. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 147).

mail/antispam/bodysizelimit

Legt die Größe der E-Mails fest, die von SpamAssassin auf Spam untersucht werden. Der Standardwert ist 300 Kilobytes. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 277).

mail/antispam/learndaily

Konfiguriert die Auswertung von Ham E-Mails im Ham-Ordner für die tägliche Auswertung. Die Auswertung ist standardmäßig aktiviert. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 277).

mail/antispam/requiredhits

Legt den Schwellenwert in Punkten fest, ab dem eine E-Mail als Spam eingestuft wird. Der Standardwert ist `5`. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 277).

mail/antivir

Um die Viren- und Schadsoftware-Erkennung für ein- und ausgehende E-Mails zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Viren- und Malwareerkennung* (Seite 278).

mail/antivir/spam

Legt fest, ob der Spam-Filter aktiv ist. Um die Spam-Filterung zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Viren- und Malwareerkennung* (Seite 278).

mail/archivefolder

Konfiguriert Postfix so, dass alle ein- und ausgehenden E-Mails zu Archivierungszwecken als Blindkopie an diese E-Mail-Adresse gesendet werden. Die Variable ist standardmäßig nicht gesetzt. Für weitere Informationen, siehe *Konfiguration einer Blindkopie zur Anbindung von E-Mail-Archivierungslösungen* (Seite 282).

mail/dovecot/auth/cache_ttl

Konfiguriert die Ablaufzeit des Authentifizierungscaches in Dovecot für den E-Mail-Dienst. Weitere Informationen finden Sie unter *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 272).

mail/dovecot/auth/cache_negative_ttl

Konfiguriert die Ablaufzeit des Authentifizierungscaches in Dovecot für den E-Mail-Dienst. Weitere Informationen finden Sie unter *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 272).

mail/dovecot/folder/ham

Legt den Namen des Ordners für E-Mails fest, die SpamAssissin als *ham* betrachtet. Der Standardwert ist `Ham`. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 277).

mail/dovecot/folder/Spam

Legt den Namen des Ordners fest, in den SpamAssissin als Spam eingestufte E-Mails verschiebt. Der Standardwert ist `Spam`. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 277).

mail/dovecot/imap

Steuert den IMAP-Protokolldienst im Dovecot IMAP-Dienst. Um den Zugriff auf E-Mails über IMAP zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Maildienste* (Seite 271).

mail/dovecot/limits

Konfiguriert verschiedene Verbindungsgrenzen für den Dovecot-Dienst. Für weitere Informationen, siehe *Beschränkung der Verbindungsanzahl* (Seite 285).

mail/dovecot/location/separate_index

Konfiguriert den Dovecot-Dienst so, dass er einen vom Speicherort der E-Mail-Nachrichten getrennten Index verwendet. Um den separaten Index zu aktivieren, setzen Sie den Wert auf `yes`. Dovecot schreibt den Index in `/var/lib/dovecot/index/`. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/mailbox/rename

Legt fest, wie die Dovecot-Dienste auf Änderungen der primären E-Mail-Adresse reagieren. Der Standardwert ist `yes` und ändert den Namen des IMAP-Postfachs des Benutzers. Für weitere Informationen über die Werte, siehe *Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten* (Seite 284).

Gemeinsame Ordner werden nicht umbenannt. Weitere Informationen finden Sie unter *Verwaltung von globalen IMAP-Ordnern* (Seite 274).

mail/dovecot/mailbox/delete

Konfiguriert die Löschung eines IMAP-Postfachs. Der Standardwert ist `no` und behält die Mailbox. Für weitere Informationen, siehe *Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten* (Seite 284).

Der Wert wirkt sich auch auf freigegebene IMAP-Ordner aus. Für weitere Informationen, siehe *Verwaltung von globalen IMAP-Ordnern* (Seite 274).

mail/dovecot/pop3

Steuert den POP3-Protokolldienst im Dovecot IMAP-Dienst. Um den Zugriff auf E-Mails über POP3 zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Maildienste* (Seite 271).

mail/dovecot/process/lock_method

Steuert die Sperrmethode für *lockd*. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/process/mail_nfs_index

Konfiguriert den Dovecot-Dienst so, dass er nach dem Schreiben von Indexdateien die NFS-Zwischenspeicher leert, wenn er auf `yes` gesetzt ist. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/process/mail_nfs_storage

Konfiguriert den Dovecot-Dienst so, dass er die NFS-Caches leert, wenn er auf `yes` gesetzt ist. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/process/mmap_disable

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/process/dotlock_use_excl

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/process/mail_fsync

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 285).

mail/dovecot/quota/warning/subject

Legt den Betreff für die E-Mail an den Benutzer fest, der die konfigurierte Quotengrenze überschreitet. Für weitere Informationen, siehe *Mail-Quota* (Seite 276).

mail/dovecot/quota/warning/text

Konfiguriert den E-Mail-Textkörper für die E-Mail an den Benutzer, der die konfigurierte Quotengrenze überschreitet. Prozentuale Werte können unterschiedliche Texte haben. Um z.B. einen Text für 50 % des Kontingents zu konfigurieren, setzen Sie `mail/dovecot/quota/warning/text/50=Ihr Text`.

Für weitere Informationen, siehe *Mail-Quota* (Seite 276).

mail/hosteddomains

Konfiguriert die von UCS verwalteten Mail-Domänen. Für weitere Informationen, siehe *Verwaltung von Mail-Domänen* (Seite 272).

mail/messagesizelimit

Legt die maximale Größe einer E-Mail in Bytes für eingehende und ausgehende E-Mails fest. Die Standardeinstellung ist `10240000` Bytes. Für weitere Informationen, siehe *Konfiguration der maximalen E-Mailgröße* (Seite 281).

mail/postfix/mastercf/options/smtp/smtpd_sasl_auth_enable

Um die Authentifizierung für die Übermittlung von E-Mails an Port 25 zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration der SMTP Ports* (Seite 282).

mail/postfix/policy/listfilter

Um den Personenkreis einzuschränken, der E-Mails an Mailinglisten senden darf, setzen Sie den Wert auf `yes` und starten Sie den Postfix-Dienst neu. Für weitere Informationen, siehe *Verwaltung von Mailinglisten* (Seite 273) und *Verwaltung von Mailgruppen* (Seite 274).

mail/postfix/postscreen/

Ein Präfix von Variablen zur Konfiguration von **postscreen**. Für weitere Informationen, siehe *Konfiguration zusätzlicher Prüfungen* (Seite 282).

mail/postfix/postscreen/enabled

Um den Postscreen für die Überprüfung der Berechtigung eingehender E-Mails zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration zusätzlicher Prüfungen* (Seite 282).

mail/postfix/smtpd/restrictions/recipient

Konfiguriert die DNS-basierte Blackhole-Liste (DNSBL) für Postfix im Format `mail/postfix/smtpd/restrictions/recipient/SEQUENCE=REGEL`.

Zum Beispiel:
`mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client ix.dnsbl.manitu.net"`.

Für weitere Informationen, siehe *Identifikation von Spam Quellen mit DNS basierten Blackhole Listen* (Seite 278).

mail/postfix/softbounce

Um E-Mails nach einem Mail-Bounce nicht zurückzusenden, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration von Softbounces* (Seite 282).

mail/postfix/tls/client/level

Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 280).

mail/relayauth

Wenn eine Authentifizierung für das Mail-Relay erforderlich ist, setzen Sie den Wert auf `yes` und fügen Sie die Anmeldedaten in `/etc/postfix/smtp_auth` ein. Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 280).

mail/relayhost

Konfiguriert den voll qualifizierten Domänennamen (FQDN) eines Mail-Relay-Servers. Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 280).

nameserver1

Definiert den ersten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

nameserver2

Definiert den zweiten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

nameserver3

Definiert den dritten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 157).

notifier/debug/level

Legt die Detailebene für die Protokollmeldungen des Notifiers in `/var/log/univention/notifier.log` fest. Die möglichen Werte reichen von 0 (nur Fehlermeldungen) bis 4 (alle Statusmeldungen). Nach einer Änderung des Debug-Levels muss der Univention Directory Notifier neu gestartet werden.

nscd/debug/level

Legt die Detailebene für Protokollmeldungen des NSCD fest. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/group/maxdbsize

Konfiguriert die Größe der Hash-Tabelle des NSCD für Gruppen. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/group/positive_time_to_live

Legt die Zeit fest, die eine aufgelöste Gruppe im Cache von NSCD gehalten wird. Die Voreinstellung ist eine Stunde in Sekunden (`3600`). Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/hosts/maxdbsize

Konfiguriert die Größe der Hash-Tabelle des NSCD für Hosts. Der Standardwert ist `6007`. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/hosts/positive_time_to_live

Legt die Zeit fest, die ein aufgelöster Hostname im Cache von NSCD gehalten wird. Die Voreinstellung ist eine Stunde in Sekunden (`3600`). Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/passwd/maxdbsize

Konfiguriert die Größe der Hash-Tabelle des NSCD für Benutzernamen. Der Standardwert ist `6007`. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/passwd/positive_time_to_live

Legt die Zeit fest, die ein aufgelöster Benutzername im Cache von NSCD gehalten wird. Die Voreinstellung ist zehn Minuten in Sekunden (`600`). Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nscd/threads

Konfiguriert die Anzahl der Threads, die NSCD verwendet. Der Standardwert ist `5`. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 173).

nss/group/cachefile/check_member

Wenn mit `true` aktiviert, prüft das Cronjob Skript zum Exportieren des lokalen Gruppen-Caches auch, ob die Gruppenmitglieder noch im LDAP-Verzeichnis vorhanden sind. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 143).

nss/group/cachefile/invalidate_interval

Legt das Intervall fest, das bestimmt, wann der lokale Gruppen-Cache als ungültig gilt und ein neuer Export durchgeführt wird. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 143).

nss/group/cachefile/invalidate_on_changes

Aktiviert oder deaktiviert den Listener, um den lokalen Gruppencache ungültig zu machen. Um den Listener zu aktivieren, setzen Sie den Wert auf `true`. Andernfalls setzen Sie den Wert auf `false`. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 143).

nssldap/bindpolicy

Steuert die Maßnahmen, die das UCS-System ergreift, wenn der LDAP-Server nicht erreichbar ist. Siehe *Name Service Switch / LDAP-NSS-Modul* (Seite 40).

ntp/signed

Der NTP-Server antwortet mit Anfragen, die von Samba/AD signiert sind, wenn der Wert auf `yes` gesetzt ist. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 174).

office365/adconnection/wizard

Definiert den Azure AD-Verbindungsalias, der bei der nächsten Ausführung des Microsoft 365-Konfigurationsassistenten verwendet wird. Für weitere Informationen, siehe *Synchronisation von Benutzern in mehrere Azure Active Directories* (Seite 214).

office365/attributes/anonymize

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365 Connector synchronisiert, aber mit zufälligen Daten füllt. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 213).

office365/attributes/mapping/.*

Definiert eine Zuordnung von LDAP-Attributen eines Benutzerkontos für die Synchronisierung mit Azure Attributen. Die Standardeinstellungen reichen in der Regel für die meisten Umgebungsanforderungen aus. Für weitere Informationen, siehe *Benutzer* (Seite 213).

office365/attributes/never

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365-Connector nie synchronisiert, auch wenn es in *office365/attributes/sync* (Seite 314) oder *office365/attributes/anonymize* (Seite 314) erwähnt wird. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 213).

office365/attributes/static/.*

Konfiguriert LDAP-Attribute für die Synchronisierung mit vordefinierten Werten. Weitere Informationen finden Sie unter *Benutzer* (Seite 213).

office365/attributes/sync

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365 Connector synchronisiert. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 213).

office365/attributes/usageLocation

Legt das Standardland für den Benutzer in Microsoft 365 fest. Die Werte sind 2-Zeichen-Abkürzungen für Länder. Weitere Informationen finden Sie unter *Benutzer* (Seite 213).

office365/debug/werror

Konfigurieren Sie zusätzliche Fehlerbehebungen für den Microsoft 365 Connector. Für weitere Informationen, siehe *Fehlersuche* (Seite 215).

office365/defaultalias

Konfiguriert den Standardverbindungsalias für Microsoft 365-aktivierte Benutzer und Gruppen. Weitere Informationen finden Sie unter *Synchronisation von Benutzern in mehrere Azure Active Directories* (Seite 214).

office365/groups/sync

Aktiviert die Synchronisierung von Gruppen der Microsoft 365-Benutzer. Um Teams zu verwenden, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Teams* (Seite 214).

password/hashing/bcrypt

Aktiviert **bcrypt** als Passworthash-Methode, wenn auf `true` gesetzt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 46).

password/hashing/bcrypt/cost_factor

Definiert den **bcrypt** Kostenfaktor und ist standardmäßig auf `12` eingestellt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 46).

password/hashing/bcrypt/prefix

Definiert das Präfix **bcrypt** und ist standardmäßig auf `2b` eingestellt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 46).

password/hashing/method

Legt die Hash-Methode für die Passwort-Hashes fest. Die Voreinstellung ist `SHA-512`. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 46).

password/quality/credit/digits

Legt die Mindestanzahl von Zeichen für ein neues Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/credit/lower

Legt die Mindestanzahl von benötigten Kleinbuchstaben im neuen Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/credit/other

Legt die Mindestanzahl der nötigen Zeichen im neuen Passwort fest, die weder Buchstaben noch Ziffern sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/credit/upper

Legt die Mindestanzahl von benötigten Großbuchstaben im neuen Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/forbidden/chars

Definiert die Zeichen und Ziffern, die für Passwörter nicht erlaubt sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/length/min

Legt die Mindestlänge für ein Passwort pro UCS-System für Benutzer fest, die nicht einer UDM-Passwortrichtlinie unterliegen. Der Wert `yes` wendet die Prüfungen der **python-cracklib** an. Der Wert `sufficient` beinhaltet keine **python-cracklib**-Prüfungen. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/mspolicy

Definiert die standardmäßigen Microsoft-Kennwortkomplexitätskriterien.

Die Werte `yes`, `1` oder `true` aktivieren die Standard Microsoft Passwortkomplexitätskriterien zusätzlich zu den anderen Kriterien, die mit **python-cracklib** überprüft werden.

Der Wert `sufficient` wendet nur die Standard Microsoft Passwortkomplexitätskriterien ohne **python-cracklib** an.

Der Standardwert ist nicht gesetzt und entspricht dem Wert `false`.

Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

password/quality/required/chars

Definiert einzelne Zeichen, die für Passwörter notwendig sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 120).

pkgdb/scan

Steuert, ob ein UCS-System Installationsprozesse im Softwaremonitor speichert. Um dies zu deaktivieren, setzen Sie den Wert `no`. Für weitere Informationen, siehe *Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor* (Seite 107).

portal/auth-mode

Legt den Authentifizierungsmodus für das UCS-Portal fest. Setzen Sie ihn auf `saml`, wenn Sie SAML für die Single Sign-On Anmeldung aktivieren wollen. Für weitere Informationen, siehe *Anmelden* (Seite 60).

portal/default-dn

Legt den LDAP-DN des Portalobjekts fest, das die Daten für das Portal enthält. Führen Sie nach der Änderung des Variablenwerts den Befehl **univention-portal update** aus. Weitere Informationen finden Sie unter *UCS Portalseite* (Seite 68).

proxy/http

Legt den HTTP-Proxyserver auf dem UCS-Hostsystem fest. Für weitere Informationen, siehe *Konfiguration des Proxyzugriffs* (Seite 159).

proxy/https

Legt den HTTPS-Proxyserver auf dem UCS-Hostsystem fest. Für weitere Informationen, siehe *Konfiguration des Proxyzugriffs* (Seite 159).

proxy/no_proxy

Legt eine Liste von Domänen fest, die nicht über einen HTTP-Proxy verwendet werden. Die Einträge werden durch Kommas getrennt. Weitere Informationen finden Sie unter *Konfiguration des Proxyzugriffs* (Seite 159).

quota/logfile

Um die Aktivierung von Quotas in einer Datei zu protokollieren, geben Sie die Datei in dieser Variablen an. Für weitere Informationen, siehe *Auswertung von Quota bei der Anmeldung* (Seite 257).

quota/userdefault

Um die Auswertung der Benutzerquoten während der Anmeldung zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Auswertung von Quota bei der Anmeldung* (Seite 257).

radius/mac/whitelisting

Um nur bestimmten Netzwerkgeräten den Zugang zu einem Netzwerk über RADIUS zu erlauben, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *MAC-Adressfilter* (Seite 242).

radius/use-service-specific-password

Um ein spezielles Benutzerpasswort für RADIUS anstelle des Domänenpassworts zu verwenden, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Dienst-spezifisches Passwort* (Seite 240).

repository/mirror/server

Legt einen anderen Repository-Server als Quelle für den lokalen Spiegel fest. Standardwert: `updates.software-univention.de`. Für weitere Informationen, siehe *Einrichtung und Aktualisierung eines lokalen Repositorys* (Seite 103).

repository/online/component/.*/unmaintained

`DEPRECATED!` Legt fest, wie mit nicht gewarteten Paketen aus zusätzlichen Repositories verfahren werden soll. Um dies zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration des Repository-Servers für Updates und Paketinstallationen* (Seite 102).

repository/online/server

Der Repository-Server, der verwendet wird, um nach Updates zu suchen und Pakete herunterzuladen. Standardwert: `updates.software-univention.de`. Für weitere Informationen, siehe *Konfiguration über Univention Configuration Registry* (Seite 103).

samba/enable-msdfs

Um das Microsoft Distributed File System (MSDFS) zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Samba neu. Für weitere Informationen, siehe *Unterstützung von MSDFS* (Seite 255).

samba/max/protocol

Konfiguriert das Dateidienstprotokoll, das Samba auf dem UCS verwendet. Die erlaubten Werte sind `NT1`, `SMB2` und `SMB3`. Für weitere Informationen, siehe *Dateidienste* (Seite 178).

samba/spoolss/architecture

Definiert die Systemarchitektur für den Druckspooler in Samba. Setzen Sie die Werte auf `Windows x64`, wenn Ihre Umgebung eine 64-Bit-Version von Microsoft Windows enthält. Für weitere Informationen, siehe *Einbinden von Druckerfreigaben auf Windows-Clients* (Seite 265).

samba4/sysvol/sync/cron

Legt das Zeitintervall für die Synchronisierung zwischen Samba/AD-Domänencontrollern für die SYSVOL-Freigabe fest. Der Standardwert ist fünf Minuten. Für weitere Informationen, siehe *Synchronisation der SYSVOL-Freigabe* (Seite 180).

saml/idp/authsource

Erlaubt Kerberos-Authentifizierung beim SAML-Identitätsanbieter. Ändern Sie auf `univention-negotiate` um zu aktivieren. Die Voreinstellung ist `univention-ldap`. Für weitere Informationen, siehe *SAML Identity Provider* (Seite 46).

saml/idp/entityID/supplement/[identifier]

Aktiviert zusätzliche lokale Identitätsanbieter für SAML auf einem UCS-System, das als UCS-Identitätsanbieter dient. Zum Aktivieren setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Erweiterte Konfiguration* (Seite 50).

saml/idp/negotiate/filter-subnets

Ermöglicht es, die Kerberos-Authentifizierung beim SAML-Identitätsanbieter auf bestimmte IP-Subnetze in der CIDR-Notation[74] zu beschränken, zum Beispiel `127.0.0.0/16,192.168.0.0/16`. Für weitere Informationen, siehe *SAML Identity Provider* (Seite 46).

saml/idp/selfservice/account-verification/error-descr

Konfiguriert den Beschreibungstext der Fehlermeldung für das **`Self Service`**. Der Text wird für Benutzer angezeigt, die sich über SSO mit einem nicht verifizierten und selbst registrierten Benutzerkonto anmelden. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 130).

saml/idp/selfservice/account-verification/error-title

Konfiguriert den Titel der Fehlermeldung für das **`Self Service`**. Der Titel wird für Benutzer angezeigt, die sich über SSO mit einem nicht verifizierten und selbst registrierten Benutzerkonto anmelden. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 130).

saml/idp/selfservice/check_email_verification

Steuert, ob die Single Sign-On Anmeldungen von nicht verifizierten und selbst registrierten Benutzerkonten verweigert wird. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 130).

security/packetfilter/disabled

Um Univention Firewall zu deaktivieren, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Paketfilter mit Univention Firewall* (Seite 236).

self-service/backend-server

Definiert das UCS-System, auf dem das Backend der Anwendung **`Self Service`** installiert ist. Weitere Informationen finden Sie unter *Passwort-Verwaltung über Self Service App* (Seite 124).

server/password/change

Aktiviert oder deaktiviert die Passwortrotation auf einem UCS-System. Standardmäßig ist die Passwortrotation aktiviert. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 147).

server/password/interval

Legt das Intervall in Tagen fest, in dem das Passwort des Computerkontos neu generiert wird. Der Standardwert ist auf 21 Tage eingestellt. Weitere Informationen finden Sie unter *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 147).

server/role

Enthält den Namen der Serverrolle des UCS-Systems. Für weitere Informationen, siehe *UCS-Systemrollen* (Seite 35).

[74] https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

squid/auth/allowed_groups

Um den Zugriff auf den Squid-Webproxy zu beschränken, definieren Sie eine Liste von Gruppennamen, die durch Semikolon (`;`) getrennt sind. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 238).

squid/allowfrom

Konfiguriert zusätzliche Netzwerke, um den Zugriff auf den Squid-Webproxy zu ermöglichen. Trennen Sie die Einträge mit Leerzeichen und verwenden Sie die CIDR-Notation, zum Beispiel `192.0.2.0/24`. Weitere Informationen finden Sie unter *Einschränkung des Zugriffs auf erlaubte Netzwerke* (Seite 237).

squid/basicauth

Um die direkte Authentifizierung für den Squid-Webproxy gegenüber dem LDAP-Server zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 238).

squid/cache

Um die Caching-Funktion des Squid-Webproxies zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Caching von Webseiten* (Seite 237).

squid/httpport

Konfiguriert den Port für Squid Web Proxy, an dem der Daemon auf eingehende Verbindungen wartet. Der Standardwert ist `3128`. Für weitere Informationen, siehe *Zugriffsport* (Seite 238).

squid/krb5auth

Um die Authentifizierung über Kerberos für den Squid-Webproxy zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 238).

squid/ntlmauth

Um die Authentifizierung für den Squid-Webproxy über die NTLM-Schnittstelle zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 238).

squid/ntlmauth/keepalive

Um weitere NTML-Authentifizierung für nachfolgende HTML-Anfragen an dieselbe Website zu deaktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 238).

squid/webports

Konfiguriert die Liste der zulässigen Ports für den Squid-Webproxy. Trennen Sie die Einträge durch Leerzeichen. Für weitere Informationen, siehe *Erlaubte Ports* (Seite 238).

sshd/permitroot

Konfiguriert, wie der SSH-Daemon die Anmeldung für den Benutzer `root` erlaubt. Der Wert `without-password` fragt nicht interaktiv nach dem Passwort. Die Anmeldung erfordert den öffentlichen SSH-Schlüssel. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 174).

sshd/port

Konfigurieren Sie den Port, den der SSH-Daemon benutzt, um auf Verbindungen zu warten. Der Standardwert ist `22`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 174).

sshd/xforwarding

Legt fest, ob der SSH-Daemon X11-Weiterleitung erlaubt. Gültige Werte sind `yes` und `no`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 174).

ssl/validity/host

Zeichnet das Ablaufdatum des Zertifikats des lokalen Computers auf jedem UCS-System auf. Der Wert gibt die Anzahl der Tage seit dem *1. Januar 1970* an.

ssl/validity/root

Zeichnet das Ablaufdatum des Stammzertifikats auf jedem UCS-System auf. Der Wert gibt die Anzahl der Tage seit dem *1. Januar 1970* an.

ssl/validity/warning

Legt den Warnzeitraum für die Ablaufprüfung des SSL/TLS-Root-Zertifikats fest. Der Standardwert ist `30` Tage. Siehe *SSL-Zertifikatsverwaltung* (Seite 44).

system/stats

Aktiviert oder deaktiviert die Protokollierung des Systemstatus. Der Standardwert ist `yes`. Für weitere Informationen, siehe *Protokollierung des Systemzustands* (Seite 171).

system/stats/cron

Legt die Laufzeiten fest, wann **univention-system-stats** ausgeführt wird. Der Wert folgt der *cron-Syntax* (Seite 172). Für weitere Informationen, siehe *Protokollierung des Systemzustands* (Seite 171).

timeserver

Konfiguriert den ersten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 174).

timeserver2

Konfiguriert den zweiten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 174).

timeserver3

Konfiguriert den dritten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 174).

ucr/check/type

Ist diese Option `Ja`, wird die Korrektheit von Typ-Definitionen und die Typ-Kompatibilität von Werten immer in Univention Configuration Registry überprüft. Bei erfolgloser Prüfung wird das Setzen des Wertes abgebrochen. Voreinstellung ist `Nein`. Für weitere Informationen, siehe *Setzen von UCR-Variablen* (Seite 163).

ucs/web/theme

Wählen Sie das Thema für UCS Web-Oberfläche. Der Wert entspricht einer CSS-Datei unter `/usr/share/univention-web/themes/` mit demselben Namen ohne Erweiterung für den Dateinamen.

umc/self-service/account-deregistration/enabled

Um die **Self Service**-Deregistrierung zu aktivieren, setzen Sie die Variable auf `True`. Weitere Informationen finden Sie unter *Selbst-Deregistrierung* (Seite 131).

umc/self-service/account-verification/backend/enabled

Aktiviert oder deaktiviert die Kontoverifizierung und die Anforderung neuer Verifizierungstokens für den **Self Service**. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 130).

users/default/administrator

Legt den Standardbenutzernamen für den Domänenadministrator fest. Der Wert kann während einer AD-Übernahme geändert werden. Für weitere Informationen, siehe *Domänenmigration* (Seite 204).

umc/http/session/timeout

Konfiguriert die Zeitspanne in Sekunden für die Browser-Sitzung, nach der das UCS-Managementsystem eine erneute Anmeldung verlangt. Der Standardwert ist `28800` Sekunden für 8 Stunden.

umc/web/oidc/enabled

Wenn mit `true` aktiviert, versucht UMC zuerst eine Single Sign-On Anmeldung über OpenID Connect, bevor es die normale Anmeldung verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 60).

umc/oidc/issuer

Konfiguriert den OIDC Identity Provider für die UMC OIDC Authentifizierung. Falls die Variable nicht gesetzt ist, wird der Wert `https://ucs-sso-ng.ucs.test/realms/ucs` verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 60).

umc/oidc/rp/server

Definiert den FQDN der *Relying Party* für UMC. Falls die Variable nicht gesetzt ist, wird der FQDN des UCS System verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 60).

umc/web/sso/enabled

Wenn mit `true` aktiviert, versucht UMC zuerst eine Single Sign-On Anmeldung über SAML, bevor es die normale Anmeldung verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 60).

16.2 Literaturverzeichnis

16.3 Stichwortverzeichnis

Das genindex bietet direkt Links zu den Inhaltsthemen. Sie enthält die Begriffe aus der Wortliste in Fettschrift.

Literaturverzeichnis

[1] *UCS documentation overview*. Univention GmbH, 2021. URL: https://docs.software-univention.de/.

[2] *Extended domain services documentation*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ext-domain/5.0/en/index.html.

[3] *Univention Developer Reference*. Univention GmbH, 2021. URL: https://docs.software-univention.de/developer-reference/5.0/en/index.html.

[4] *Univention Keycloak app documentation*. Univention GmbH, 2023. URL: https://docs.software-univention.de/keycloak-app/latest/.

[5] *UCS performance guide*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ext-performance/5.0/en/index.html.

[6] *Extended installation documentation*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ext-installation/5.0/en/index.html.

[7] *Extended Windows integration documentation*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ext-windows/5.0/en/index.html.

[8] *Group Policy ADMX Syntax Reference Guide*. Microsoft, July 2021. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753471(v=ws.10)?redirectedfrom=MSDN.

[9] *How to Implement the Central Store for Group Policy Admin Templates, Completely (Hint: Remove Those .ADM files!)*. Microsoft, September 2018. URL: https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/how-to-implement-the-central-store-for-group-policy-admin-templates-completely-h/255448.

[10] Microsoft, editor. *Windows Server 2003/2003 R2*, chapter WMI filtering using GPMC, pages 18372f. Microsoft, January 2005. URL: https://www.microsoft.com/en-US/download/details.aspx?id=53314.

[11] Mark Heitbrink. *Filtern von Gruppenrichtlinien anhand von Benutzergruppen, WMI und Zielgruppenadressierung*. January 2013. URL: https://www.gruppenrichtlinien.de/artikel/filtern-von-gruppenrichtlinien-anhand-von-benutzergruppen-wmi-und-zielgruppenadressierung/.

[12] *Installieren der Zertifizierungsstelle*. Microsoft, März 2023. URL: https://learn.microsoft.com/de-de/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority.

[13] Cricket Liu and Paul Albitz. *DNS and BIND*, chapter 12 Reading BIND Debugging Output, pages 502. O'Reilly, 3rd edition, September 1998. URL: https://www.diablotin.com/librairie/networking/dnsbind/ch12_01.htm.

[14] *Extended IP and network management documentation*. Univention GmbH. URL: https://docs.software-univention.de/ext-networks/5.0/en/index.html.

[15] Jelmer R. Vernooij, John H. Terpsta and Gerald (Jerry) Carter. *The Official Samba 3.2.x HOWTO and Reference Guide*, chapter 20 - Hosting a Microsoft Distributed File System Tree, pages 381–384. Samba Project, May 2009. URL: https://www.samba.org/samba/docs/Samba3-HOWTO.pdf.

[16] *Univention OX Connector app documentation*. Univention GmbH, 2023. URL: https://docs.software-univention.de/ox-connector-app/latest/.

Stichwortverzeichnis

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V